Next Generation Enterprise Network: Network Operations (NetOps) Concept of Operations (CONOPS)

7 April 2008

Letter of Promulgation

1. The Next Generation Enterprise Network (NGEN), Network Operations (NetOps) Concept of Operations (CONOPS) is approved for implementation. The document is "Source Selection Sensitive" and classified " Safeguard in accordance with the Department of the Navy (DON) Information Security Program Regulation.
2. NetOps CONOPS identifies how the DON intends to operate and defend NGEN. It also provides a foundation for the development of future NetOps CONOPS; standard operating procedures; and tactics, techniques, and procedures (TTPs).
3. NGEN is the replacement for today's Navy-Marine Corps Intranet (NMCI) and will be implemented in spiral fashion. NGEN Block 1, starting in October 2010, will provide as a minimum current capabilities and services of NMCI. Final state of NGEN will enable the DON to achieve its long term Net-Centric goals.
4. This document shall be reviewed and/ or updated annually by Commander, Naval Network Warfare Command and Commanding Officer, Marine Corps Network Operations and Security Center.
5. Distribution authorized to the Department of Defense (DoD) personnel and U.S. DoD contractors that have signed appropriate non-disclosure agreements.

_____

Director, Command, Control, Communications, and Computers

Department of the Navy Deputy Chief Information Officer for U.S. Marine Corps

_____

Commander, Naval Network Warfare Command

_____

Deputy Chief of Naval Operations for Communication Networks

Department of the Navy Deputy Chief Information Officer for U.S. Navy

Table of Contents

1 Executive Summary

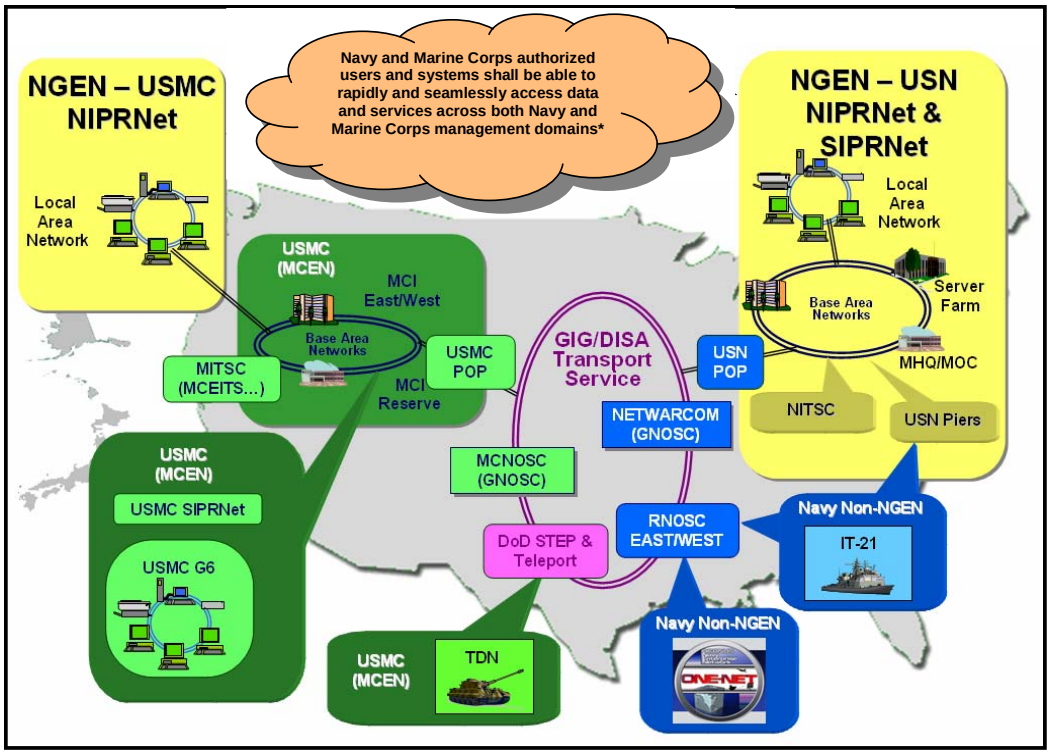
1.1 Purpose

The purpose of this Network Operations (NetOps) concept of operations (CONOPS) is to outline how the Department of the Navy (DON) intends to operate and defend the Next Generation Enterprise Network (NGEN) at full operational capability (FOC). NetOps encompasses all activities associated with operating and defending networks, their applications, and their services. This CONOPS supports the naval acquisition community in the development of capabilities needed for NGEN NetOps. Additionally, it will serve as the foundation for the development of future NGEN CONOPS; standard operating procedures; and tactics, techniques, and procedures (TTPs).

1.2 What is Next Generation Enterprise Network (NGEN)?

NGEN is an acquisition program whose initial objective is to replace today's Navy-Marine Corps Intranet (NMCI) – which currently provides approximately 320,000 seats to both U.S. Navy (USN) and U.S. Marine Corps (USMC) users. The initial block of NGEN must be able to provide a follow-on capability for NMCI seats and services after the expiration of the NMCI contract. Figure 1 shows the OV-1 for NGEN Block 1, which provides a description of the interactions between the NGEN Block 1 architecture and its environment.

Figure 1: OV-1 for NGEN Block 1



*Identified requirement is not meant to infer that NGEN must be a single physical network.

1.3 Network

A network is multiple connected computers that communicate over a wired or wireless medium to share data, as well as other resources, and are under the control of a Service component command authority. A network represents the totality of voice, video, and data services infrastructure from wide area network to desktops.

The command authorities for the USN and USMC networks are:

- **Naval Network Warfare Command (NETWARCOM)**. The Commander, NETWARCOM is the USN Component Commander for the Joint Task Force (JTF) – Global Network Operations (GNO).
- **Marine Corps Network Operations and Security Center (MCNOSC)**. The Commandant of the Marine Corps (CMC) exercises Service command of the Marine Corps Enterprise Network (MCEN) through the Director C4 and the Commanding Officer, MCNOSC, who has been delegated command authorities to operate and defend the MCEN. The Commanding Officer, MCNOSC is also the USMC Component Commander for JTF-GNO.

NETWARCOM and MCNOSC, as Component Commanders for JTF-GNO, exercise operational control (OPCON) over the USN and USMC networks, respectively.

1.4 NGEN Management Domains

Management Domains (MDs) are boundaries within a network for which a management authority will effect command and control. MDs in the Navy are designated by the network's Service component command authority (NETWARCOM) and in the Marine Corps by Director C4. MDs include within them the ability to direct and manage network resources and capabilities.

NGEN NetOps functions will be exercised via two separate NGEN MDs – one for the USN and another for the USMC:

- **USN NGEN MD**. NETWARCOM shall operate a NGEN MD that supports roughly 235,000 seats for USN users.
- **USMC NGEN MD**. MCNOSC shall operate a NGEN MD that supports roughly 85,000 unclassified seats for USMC users.

Two separate MDs allow both NETWARCOM and MCNOSC to operate their respective components of NGEN in a manner best suited to support the different operational objectives, mission priorities, and business processes of the USN and USMC, respectively, as well as meet their JTF-GNO Component Commander obligations.

1.5 Global, Regional, and Local NetOps Relationships

This CONOPS outlines the OPCON, tactical control (TACON), and supported/supporting relationships that will be used by NETWARCOM and MCNOSC to support the operation and defense of their respective NGEN MDs. A command and control (C2) structure is needed to define these relationships and the concepts of:

- **Global NetOps**. IT services and functions shall be managed globally where appropriate to minimize IT workforce requirements and maximize global responsiveness.
- **Regional NetOps**. Deployed/tactical commands and users require a more de-centralized management structure to allow them to be responsive to the regional priorities of the Commander.
- **Local NetOps**. USN detachments and USMC Base G6s subordinate to a regional/global NetOps authority shall manage local services on the behalf of supported commands.

The concept of global, regional, and local NetOps authorities outlined in this CONOPS strikes a balance between the need for global end-to-end management and the operational flexibility of regionally or locally delivered support. All global, regional, and local NetOps authorities will be elements of either the NETWARCOM or MCNOSC command structure and their authorities will be delineated by OPCON and TACON relationships. The intent of this NetOps C2 structure is to entrust regional and local NetOps commanders with the operational flexibility to accomplish their mission and to improve responsiveness and flexibility within the MD while not jeopardizing global operations and priorities.

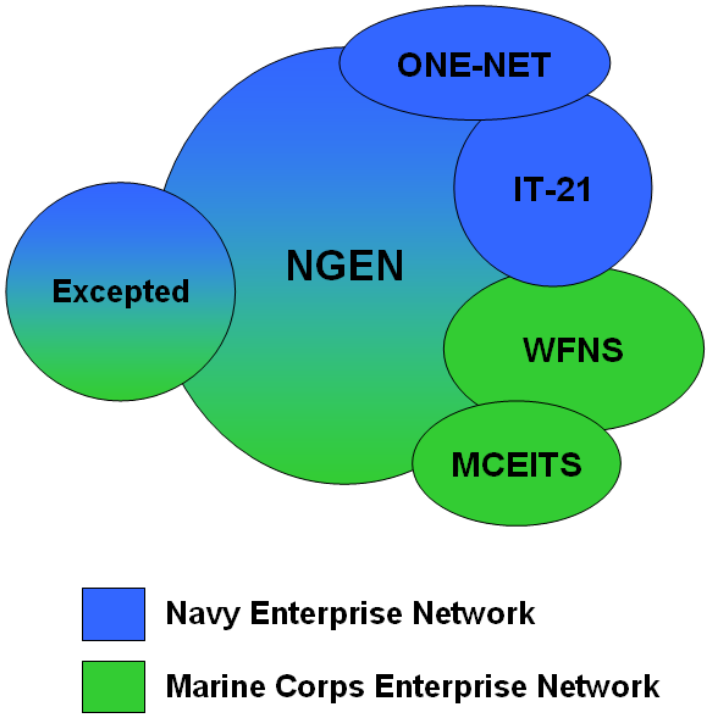
2 Key NGEN Concepts

This section outlines the key concepts for NGEN NetOps, which are consistent with the draft *Department of Defense NetOps Strategy* and *Global Information Grid NetOps CONOPS*.

2.1 Naval Networking Environment

The Naval Networking Environment (NNE) includes all of the networks used by the DON in support of operational and business objectives. The NNE ensures networks are interoperable through use of common standards and architectures. Figure 2 shows how NGEN relates to other net-centric capabilities and is a key component of the future NNE.

Figure 2: Future Naval Networking Environment



2.2 Networks

- **Navy Enterprise Network**. The Commander, NETWARCOM is the Service component command authority for the Navy Enterprise Network. The Commander, NETWARCOM is also the USN Component Commander for JTF-GNO.
- **MCEN**. The CMC exercises Service command of the MCEN through the Director C4 and further delegated command authorities to the Commanding Officer, MCNOSC, who has been assigned the mission to operate and defend the MCEN. The Commanding Officer, MCNOSC is also the USMC Component Commander for JTF-GNO.

2.3 Management Domains

MDs are the boundaries within a network for which a management authority will affect operational level C2. MDs are designated by NETWARCOM or Director C4 and include within them the ability to direct and manage network resources and capabilities.

2.3.1 USN MDs

The USN will have the following MDs:

- **Information Technology for the 21st Century (IT-21)**. IT-21 consists of the shipboard LANs, satellite communications programs, and a shore-based infrastructure (i.e., Tactical Switching) to support IT services for the fleet. The Consolidated Afloat Networks and Enterprise Services (CANES) is a program of record that will replace existing shipboard IT services.
- **OCONUS Navy Enterprise Network (ONE-NET)**. ONE-NET provides a single integrated network with a full range of services and a centralized control authority for installations overseas.
- **NGEN**. NMCI currently supports roughly 235,000 seats, which will be transitioned into NGEN, for USN installations and users in the U.S.
- **Excepted**. Cyber Asset Reduction and Security (CARS) is a USN Task Force charged with identifying and implementing consistent, secure solutions for legacy systems and reduce the number of legacy systems that are not a part of the USN MDs discussed above. USN legacy systems that meet approved criteria will be given an excepted status by CARS and be operated as their own MD.

2.3.2 USMC MDs

The USMC will have the following MDs:

- **NGEN**. NMCI currently supports roughly 85,000 unclassified seats, which will be transitioned into NGEN, for USMC installations and users in the U.S.
- **Marine Corps Enterprise IT Services (MCEITS)**. A proposed program of record that will develop an application and services hosting capability as well as support DOD enterprise services. MCEITS Enterprise IT Centers (EITCs) will host enterprise-class applications/services required by the supporting establishment and the warfighter. Regional MAGTF IT Support Centers (MITSCs) will host regional-class/local applications and provide services used by MAGTFs. In addition to provisioning the EITCs and regional Distributed Hosting Platforms, MCEITS will develop the IT services that will be hosted at these facilities as well as leverage DOD enterprise services that lend themselves to presentation within MCEITS.

- **Warfighter Network Services (WFNS)**. A proposed program of record that will spawn multiple CPDs. WFNS will provide for the extension of the MCEN (both classified and unclassified) to support MAGTFs and their components in the conduct of military operations and exercises by provisioning the capability to instantiate, operate, maintain, and defend highly-scalable, tactical networks for deployed Marines in support of the full range of military operations. As authorized by the Secretary of the Navy, WFNS will also provide the USMC with its garrison SIPRnet capability and services to ensure it maintains the ability to prepare and support Marine Forces engaged in military operations and exercises. Finally, WFNS will upgrade, consolidate and provide for operational support and management for non-NMCI/non-NGEN unclassified network infrastructure.

2.3.3 DOD MDs

The Department of Defense (DOD) will have the following MDs:

- **Defense Information Systems Network (DISN) Core**. A program that consolidated all DOD packet-based WAN services into the NIPRnet and SIPRnet. The DISN Core is acquired, operated, and managed by the Defense Information Systems Agency (DISA). DOD enterprise-class services, such as Net-Centric Enterprise Services, will be provided via the DISN Core.

2.4 Community of Interest

A community of interest (COI) is a group of users that collaborate in support of a common operational (e.g. Surface Warfare, Amphibious Operations, Joint Task Force, etc.) or functional (e.g., logistics, personnel, medical, training, etc.) objective. A COI can include users from a single MD, multiple MDs, network, or multiple networks. A number of different COIs will be supported by the NNE.

2.5 What are Operations in Cyberspace?

Cyberspace is an evolving concept for an emerging warfighting domain. For the purposes of this CONOPS, cyberspace is defined as the hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to operate.[1] Traditional functions of warfare – maneuver, intelligence, fires, force protection, logistics, and C2 – are applied to operations within the land, maritime, air, and space domains. As cyberspace increases in importance from a force multiplier to a major warfare domain, traditional elements of warfare must be considered in accomplishing cyber objectives:

- **Maneuver**. Maneuver is the movement to place ships, aircraft, or land forces in a position of advantage over the enemy. Maneuver within cyberspace is the marshaling of network resources (e.g., transport services, storage services, processing power, personnel, etc.) to create an information advantage over an adversary. Maneuver includes the ability to change the readiness level of the network through INFOCON to achieve position of advantage over a potential attacker.

---

[1] *National Strategy to Secure Cyberspace*, February 2003.

- **Develop Intelligence**. Intelligence is information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. Intelligence within cyberspace is information or knowledge about an adversary's information systems, networks, their disposition, and their intentions against our own cyberspace capabilities.
- **Conduct Fires**. Fires are the effects of lethal or non-lethal weapons. Fires within cyberspace are the employment of network attacks (e.g., Trojans, computer viruses, malicious code, denial-of-service attacks, etc.).
- **Perform Logistics**. The science of planning and carrying out the movement and maintenance of forces. Logistics within cyberspace is the planned movement and maintenance of information systems (e.g., computers, switches/routers, software, etc.), personnel (e.g., systems administrators, knowledge managers, etc.), and IT services (e.g., e-mail, file storage, capacity, etc.).
- **Provide Force Protection**. Force protection constitutes actions taken to prevent or mitigate hostile actions against U.S. forces (i.e., personnel, resources, facilities, and critical information). Force protection within cyberspace encompasses capabilities (e.g., encryption, firewalls, network scanning and disinfection services, physical protection, redundancy, etc.) and actions (e.g., information control procedures, data recovery, contingency plans, etc.) required to prevent or mitigate hostile or non-hostile (e.g., natural disaster) actions against critical data and information systems. Cyber force protection must ensure a gradual – as opposed to catastrophic – degradation of cyber capabilities.
- **Exercise C2**. C2 is the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission. C2 within cyberspace is the exercise of authority and direction by a commander over assigned cyber resources (i.e., the cyberspace equivalents of maneuver, intelligence, fires, force protection, and logistics). Cyberspace C2 implies visibility, monitoring, management, and reallocation of all cyberspace resources to achieve cyberspace objectives and support the accomplishment of the mission.

NetOps is the joint concept for accomplishing cyber objectives by responsively operating and defending networks, their applications, and their services. However, NetOps does not include offensive actions, such as cyber fires, or exploitation, such as the development of cyber intelligence.

2.6 What is NetOps?

NetOps is an operational construct used by the Commander, United States Strategic Command (USSTRATCOM) to operate and defend the DOD's GIG. NetOps encompasses all activities associated with operating and defending networks, their applications, and their services. The objective of NetOps is to rapidly provide decision-makers with contextual information that allows them to make well-informed decisions that can quickly be passed to their forces for action. To accomplish this, NetOps requires shared situational awareness as well as the technologies, procedures, tools, and collaborative organizational structures to rapidly assess and respond to system and network degradations, outages, or changes in operational priorities.

NetOps mission essential tasks are:

- **Enterprise Management (EM)**. The management (fault, configuration, performance, planning, etc.) of communications (terrestrial and space), electromagnetic spectrum, computer-based information systems, elements of systems, and services to include software applications.
- **Network Defense (ND)**. Includes the following activities:
  - *Information Assurance (IA)*. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
  - *Computer Network Defense (CND)*. Defensive measures to protect, monitor, analyze, detect, and respond to unauthorized activity with DoD information systems and computer networks and defend information, computer, and networks from disruption, denial, degradation, or destruction. CND employs IA capabilities in response to CND alert or threat information.
  - *Computer Network Defense Response Actions (CND RA)*. Deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks under attack or targeted for attack by adversary computer systems/networks.
  - *Critical Infrastructure Protection (CIP)*. Actions taken to prevent, remediate, or mitigate the risks resulting from critical infrastructure vulnerabilities. Actions could include changes in TTPs; adding redundancy; selection of another asset; isolation or hardening; guarding; etc.
- **Content Management (CM)**. Adjusts information delivery methods and priorities for enhanced situational awareness, and allows information producers to advertise, publish and distribute information. CM is accomplished by enabling users to safeguard, compile, catalog, discover, cache, distribute, retrieve and share data in a collaborative environment.

In addition to the above mission essential tasks, the concepts of situational awareness and C2 are essential to the NetOps framework and are required upon NGEN initial operating capability (IOC):

- **Situational Awareness**. An enabling capability of NetOps is achieving shared situational awareness of the status of the network, its services, and its applications. Situational awareness improves the quality and timeliness of collaborative decision-making regarding the employment, protection and defense of the network and, therefore, is a key enabler of C2. NetOps situational awareness is achieved by the following functions:
  - *Visibility*. NetOps requires a real-time awareness of the "status" of its IT services infrastructure.

- *Monitoring and Analysis*. NetOps requires the ability to receive status and performance related information about the resource and provide discrete analysis, assess current or potential impact to warfighting and warfighting support missions, determine course of action alternatives, etc.

- **Command and Control (C2)**. Given the inherent global reach of a network, many NetOps activities may not be under the same command authority and C2 processes are needed to ensure unity of effort. The following NetOps C2 activities support the global integration of NetOps, across widely dispersed network operations centers, to operate and defend the network in a manner consistent with operational priorities across the range of military and business operations:
  - *Planning*. Planning establishes procedures and parameters for contingencies. It also establishes levels of operational control and delegated authorities for each organization involved in a specific operation or theater of action. Finally, planning evaluates current and past performance to gain lessons learned and to improve the planning process for future operations.
  - *Coordinating/Responding*. NetOps requires processes for quickly creating common action, movement, or condition among different elements to achieve the most effective results through unified and harmonious action. Coordination is inherent in command and can be one of the most important capabilities of a commander employing the "centralized planning, decentralized execution" command style. Responding is the process of quickly reacting to stimulation and reacting appropriately to achieve the most effective results while preserving the integrity of the network.
  - *Management*. NetOps requires the ability to make decisions concerning the installation, operation, and/or maintenance of available IT service infrastructure. It consists of those continuing actions of planning, organizing, directing, coordinating, controlling, and evaluating the use of personnel, money, materials, and facilities to accomplish missions and tasks.
  - *Control*. NetOps requires the ability to direct and manage available resources, or allocate them to specific missions. The ability to exert control over these resources enables command functions, which is the ability to direct changes to resources as necessary to achieve a desired result within a specified timeframe.

3 NGEN NetOps Requirements

This section summarizes the NetOps requirements for NGEN based on the *Operational Control Strategy Focus Area, NGEN Requirements Document*, and draft *Department of Defense NetOps Strategy*.

3.1 NGEN NetOps Requirements

- **Visibility into the health and status of NGEN operations**. It will not be possible for the DON to execute NetOps without an understanding of the status and health of the network. To improve visibility into the status and health of NGEN, the DON requires:
  - *Near real-time system and service status information*. NGEN must provide appropriate performance metrics for its systems and services in near real-time. This information is needed to support the development of consistent operational pictures of the status of NGEN.
  - *Historical data on system and service usage*. NGEN must provide historical performance data for trend analyses to support capacity planning, service valuation, etc.
  - *Threat and vulnerability status information*. The DON is obligated to report threat and vulnerability information to the Joint Task Force (JTF) – Global Network Operations (GNO). This information is also needed to support the development of a consistent security picture.
  - *Ownership of and access to all necessary performance data*. The vendor may collect, store or archive data on behalf of the DON, but the DON owns the data and requires easy access to it. The vendor will not fail to collect or delete agreed upon data without prior approval from the DON.
  - *Ability to display consistent operational pictures of the status of NGEN*. Consistent operational pictures are needed for reporting the status, threat, vulnerability, and mission impact of degradation to both NetOps and operational commanders in a manner tailored to their areas of responsibility/interest.
  - *Ability to obtain and display information from JTF-GNO, other Services, DISA, etc. regarding the health and status of their networks*. NGEN needs visibility into the status of other networks, their current threat environment, etc. to provide situational awareness into problems or threats which may impact NGEN and allow its NetOps commanders to take proactive measures to address them.
- **Alignment of operational and contractual authorities**. During high tempo operations, NGEN resources will be in high demand. As a result, direction from operational commanders is necessary to prioritize demands, especially during network outages, security events, and changing mission requirements. To ensure NGEN is both responsive and agile, the DON requires:

- *Vendor resources be clearly linked to NetOps authorities*. Vendor-managed NetOps resources and capabilities must be assigned to a DON NetOps authority responsible for organizing and employing these resources, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission.
- *Vendor resources must be responsive to the NetOps authorities to which they are assigned*. Vendor resources subordinate to a DON NetOps authority must be responsive to that operational authority. This is especially critical when available vendor resources are limited and demand for them is high.

- **Alignment of resources with military organizations and missions**. Control of NGEN resources for day-to-day operations should be assigned at the global, regional, and/or local level in accordance with the responsiveness, adaptability, and survivability requirements of the users/missions the resources support. To ensure NGEN is both mission oriented and user focused, the DON requires:
  - *Security services be globally controlled and managed*. The DON needs to maintain global control over security services to remain responsive to JTF-GNO directions.
  - *Standardized, shared data environment may be managed regionally or locally*. Resources that support various COIs can be managed either regionally or locally to ensure each COI is responsive to the needs and missions of its users.
- **Development of tools and processes to exercise C2 over NGEN resources**. NGEN must provide a complete suite of C2 tools to support the processes through which properly designated NetOps commanders exercise authority and direction over assigned and attached forces or capabilities. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a NetOps commander in planning, directing, coordinating, and controlling NGEN resources in the accomplishment of warfighting and warfighting support missions. To ensure unified C2 over NGEN resources, the DON requires:
  - *Common set of reporting, planning, and execution tools for the vendor and the DON*. A common set of tools and interfaces are needed to execute the EM, ND, and CM NetOps mission essential tasks.
  - *Common set of reporting and planning tools for the DON and JTF-GNO, other Services, DISA, COCOMs, etc*. In a networked world, any problem in one network can affect all of the other networks connected to it. Consequently, NetOps commanders from networks that span different DOD agencies and Services need to be able to share information and coordinate their responses to quickly address emerging threats.
  - *Interoperable trouble ticket management system for the vendor and the DON*. Both the vendor and the DON need to use an interoperable trouble ticket system to track NGEN trouble tickets. The capability to transfer and track trouble tickets between MDs and networks is essential to rapid response to operational tasking and resolution of incidents and problems.

- **Focus on network defense activities**. Security is a top priority for the DON and the NGEN contract must be structured in a manner that ensures network defense activities are a top priority of the vendor. To ensure the security and integrity of NGEN resources and services as well as DON data and processes, the DON requires:
  - *Compliance with DON and DOD security requirements*. NGEN must comply with current DON and DOD IA/IT security policies and instructions.
  - *Responsiveness to emerging security threats*. Network security threats are constantly evolving as new exploits and attacks are developed to counter network defense activities. ND activities on NGEN must be able to respond to these threats within timelines of minutes, hours, or days depending on the nature of the threat. A globally integrated and managed state of the art sensor grid, INFOCON management and readiness reporting, and scanning tools provide the highest levels readiness, minimize vulnerabilities, and ensure rapid detection and response to threats on a global scale.
  - *Archiving of log files to support forensic analyses of penetrations*. When a penetration is discovered, log files and the tools/personnel to analyze them are needed to support the forensic analyses that reconstruct the attack vector used to penetrate NGEN. These forensic analyses will be critical to modifying TTPs, SOPs, and NGEN services to detect, mitigate, and eliminate vulnerabilities.
- **Support the full range of continuity of operations (COOP) activities**. Events – such as operator error, natural disasters, hostile attacks, etc. – will degrade the network. To ensure COOP, the DON requires:
  - *Service redundancy and failover appropriate to the supported missions*. Large, high-impact service outages are a result of centralizing services without an adequate COOP capability. For services that support critical operations, such as management services or missions, high availability and redundancy are needed to ensure services are available during high tempo operations or when an adversary is actively attempting to disrupt or degrade NGEN capabilities.
  - *Degradation of services by request*. NetOps commanders and operators must practice implementing contingency plans, in response to NGEN degradations, to ensure COOP during an actual event. Service contracts should have provisions that allow the DON to request the degradation of services in support of COOP exercises and training. For example, intentionally degrading service performance (i.e., systems going offline, loss of bandwidth, etc.) during an exercise provides NetOps commanders the opportunity to train operators how to recognize, respond, and continue to function during a network attack.

3.2 NGEN NetOps-Driven Capabilities

These NetOps requirements drive the following NGEN capabilities:

- **Shared situational awareness**. Provide NGEN users, operators, and commanders at all levels with accurate and timely information which enables a shared understanding of the health and mission readiness of NGEN.
- **Responsiveness and agility**. Rapidly changing and unanticipated mission priorities and requirements can be met by dynamically maneuvering NGEN resources.
- **Mission oriented**. All information dependent processes necessary for a mission can be effectively supported.
- **User focused**. Users have secure access to obtain needed information at anytime and from anywhere in a timely manner – even when their needs are unanticipated.
- **Unified C2**. Adopt a unified NGEN C2 approach for the proactive operation and defense of NGEN – even with multiple MDs.
- **IA/CND**. Provide a secure NGEN network operating and IT services environment for all NGEN users.

4 NGEN NetOps Relationships

This section summarizes NGEN NetOps relationships based on guidance from the *Navy NetOps CONOPS* and *USMC Integrated Communications Strategy*. Traditional C2 terminology, as defined in *Joint Publication 3-0: Joint Operations*, will be used to describe global, regional, and local NetOps functions.

4.1 NetOps C2 Relationships

A C2 structure is required to exercise NetOps control over DON network resources in support of the accomplishment of warfighting and warfighting support functions. Therefore, OPCON and TACON command relationships are needed to support NetOps. As outlined in Joint doctrine, operational relationships (COCOM, OPCON, TACON, and Support) are established between or delegated to Commanders and not primary staff members or operations centers. For simplicity, language in the following chapters often indicate or infer delegated authorities to N-6/G-6, OPCON/TACON over RNOSC/ITSC and other operations centers, or supporting relationships with commands and users. However, in reality, these formal C2 relationships exist between the various commanders of the units within which the personnel (N-6/G-6 staff), operations centers (GNOSC/RNOSC/ITSC), and technical capabilities to execute NetOps exist, as well as with the commanders of the units they support.

4.1.1 NetOps OPCON

OPCON is command authority that may be exercised by commanders at any echelon at or below the level of combatant command. OPCON is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. OPCON includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. OPCON should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. OPCON provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training.

NetOps OPCON involves:

- **Delineate NetOps functional/geographic responsibilities**. Establishing NetOps supporting relationships, shifting supporting responsibilities between network operations centers when operational forces deploy from one region to another, etc.
- **Assigning NetOps tasks and objectives**. Prioritizing response to network incidents or outages, etc.
- **Giving authoritative NetOps direction**. Directing how network and service resources will be apportioned, mandating certain system configuration settings, establishing information condition, etc.

- **Delegate NetOps TACON**. Delegating authority to the subordinate forces necessary to accomplish the tasks and objectives assigned to them.

4.1.2 NetOps TACON

TACON is command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. TACON is inherent in OPCON. TACON may be delegated to, and exercised at any level at or below the level of combatant command. TACON provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task.

NetOps TACON involves:

- **Detailed NetOps direction**. Determine how apportioned resources will be allocated, changes to system configuration settings will be implemented, implementing global information condition, setting local information condition as needed, etc.
- **Control of NetOps maneuvers**. Determine which systems need to be isolated/re-baselined in response to a network incident, provide users with network access, determine their level of access, allocate resources on the network, determine who can access their content, etc.

4.1.3 NetOps Supporting Relationships

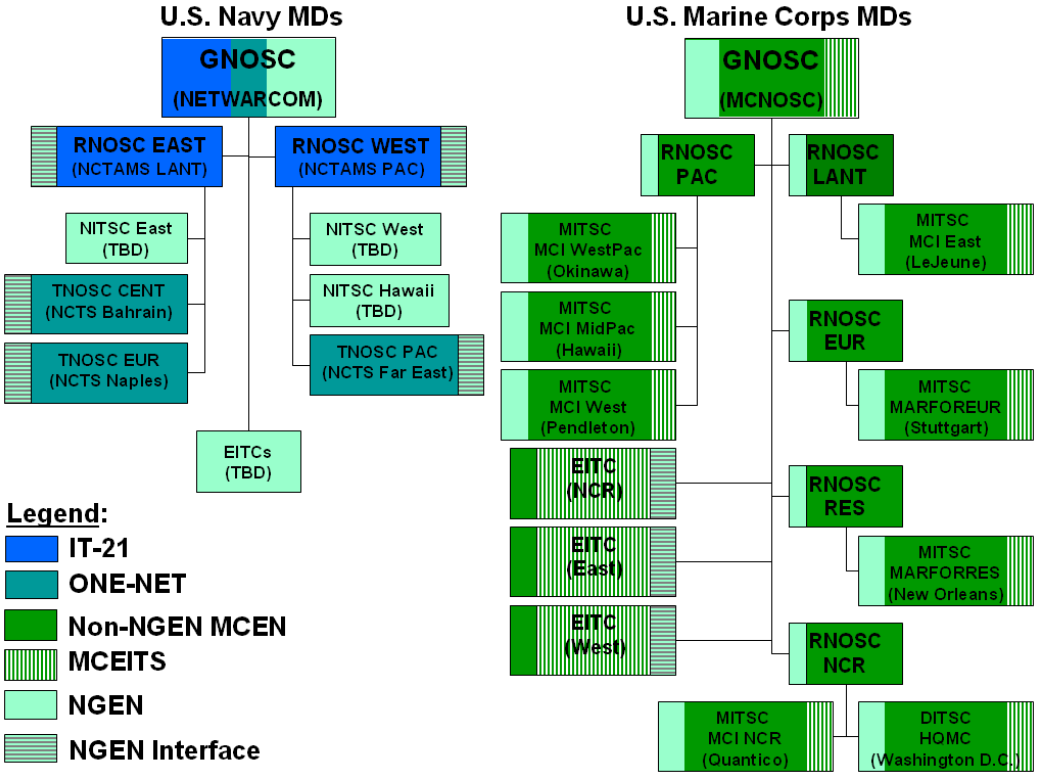
Commands with NetOps responsibilities operate and defend these networks on the behalf of the commands they support, who require net-centric capabilities to support their daily operations. There is an inherent supporting-supported relationship between the NetOps and operational (i.e., warfighting or warfighter support) commands.

4.2 NetOps in the Naval Networking Environment

Figure 3 depicts the NetOps relationships of the NNE, which spans multiple networks and MDs. The NetOps criteria for the operation of the NNE are driven by the following:

- **Global NetOps**. IT services and functions shall be managed globally whenever possible to minimize IT workforce requirements and maximize global responsiveness.
- **Regional NetOps**. Deployed/tactical commands and users require a more de-centralized management structure to allow them to be responsive to the regional priorities of the Commander. Furthermore, in a deployed/tactical environment, users may suffer from bandwidth limitations and intermittent connectivity, which may require different applications and services optimized for their environment. Regional Network Operations and Security Centers (RNOSCs), Theater Network Operations and Security Centers (TNOSCs), Navy IT Support Centers (NITSCs), and MAGTF Information Technology Support Centers (MITSCs) will support regional NetOps.
- **Local NetOps**. USN detachments and USMC Base G6s subordinate to a regional/global NetOps authority shall manage local services on the behalf of supported commands. Mobile/tactical users may need greater autonomy if expected to operate while disconnected from the larger network.

Figure 3: NetOps in the Naval Networking Environment



4.3 USN NGEN Management Domain

This section describes the global, regional, and local NetOps authorities responsible for the operation and defense of the USN NGEN MD.

4.3.1 Global NetOps

NETWARCOM shall operate the Global Network Operation and Security Center (GNOSC) for the USN NGEN MD and exercise global NetOps OPCON over it. NETWARCOM is the Navy's central operational authority for space, IT requirements, network and information operations in support of naval forces afloat and ashore. The Commander, NETWARCOM, via the USN GNOSC, will have the following NGEN responsibilities:

- **Establishing and, when necessary, shifting NetOps supporting relationships between regional NetOps authorities**. NETWARCOM is responsible for re-assigning support relationships. For example, NETWARCOM could re-assign supporting responsibilities when operational forces deploy from one region to another or in response to operational/network events.
- **Providing authoritative direction needed to coordinate global functions**. Certain management functions, such as security, need to occur on a global scale. NETWARCOM shall provide the authoritative direction needed for services that require global management.

- **Assigning tasks and objectives in response to global network events**. NETWARCOM shall respond to global network events by establishing priorities and assigning tasks and objectives to subordinates to accomplish them in conjunction with JTF-GNO and Fleet authorities.

USN EITCs are data centers that will host enterprise-class applications/services required by the supporting establishment and the warfighter. USN EITCs will be subordinate to the USN GNOSC, who is responsible for directing and coordinating global functions.

4.3.2 Regional NetOps

Each RNOSC is a functional component of a NCTAMS and shall exercise regional NetOps OPCON, as delegated by the Commander, NETWARCOM, over the USN NGEN MD by:

- **Responding to direction and tasking from the USN GNOSC**. NETWARCOM maintains global NetOps OPCON over the USN MD and each RNOSC is subordinate to it.
- **Providing authoritative direction needed to coordinate regional operations**. The RNOSC shall provide the authoritative direction needed for regional management functions.
- **Assigning tasks and objectives in response to regional network events**. The RNOSC, in coordination with the Geographic Combatant Command and the Naval Component Commander shall establish regional priorities and assign tasks and objectives to subordinates.
- **Managing NGEN resources for supported commands and users**. The RNOSC is responsible for managing its resources on behalf of the commands/users it is responsible for supporting.

The RNOSC shall delegate appropriate authorities to NITSCs to support regional NetOps capabilities, which is analogous to the existing NCTAMS-NCTS structure used by the IT-21 and ONE-NET MDs. Each NITSC will be a subordinate element of the RNOSC.

4.3.3 Local NetOps

Local detachments will be subordinate elements of a RNOSC/NITSC and shall exert NetOps TACON over its designated area of responsibility by:

- **Responding to direction and tasking from the GNOSC, RNOSCs, and NITSCs**. The local NetOps authority shall respond to tasking and direction from higher NetOps authorities.
- **Managing access control for supported commands**. The local NetOps authority shall support the management of access to NGEN.
- **Managing all locally hosted services and applications**. Some services and applications might be hosted and/or managed by the local NetOps authority.

Deployable commands – such as strike group, destroyer squadron, and air squadron staffs – will be delegated greater local NetOps authority when deployed and their NetOps support relationship will shift to the appropriate NetOps authority (e.g. RNOSC/TNOSC).

4.3.4 Summary of the USN MD

The NetOps C2 relationships outlined in this section strike a balance between the need for global end-to-end management and the operational flexibility of regionally or locally delivered support. The GNOSC delegates some NetOps authority to the RNOSCs, who then delegate some authority to NITSCs, to support regional NetOps capabilities that are more responsive to the needs of operating forces. The global and regional NetOps authorities also delegate some NetOps authority to detachments to support local NetOps capabilities that are more responsive to the needs of individual commands. The intent of this NetOps C2 structure is to delegate some authorities to regional and local NetOps authorities to improve responsiveness and flexibility within the MD while not jeopardizing global operations and priorities.

All DoN commands, including the Secretariat and the COCOMs, have a NetOps supported-supporting relationship with a regional NetOps authority. Figure 4 summarizes the global, regional, and supported-supporting C2 relationships for NetOps in the USN NGEN MD.

Figure 4: NetOps C2 and Support Relationships for the USN NGEN Management Domain

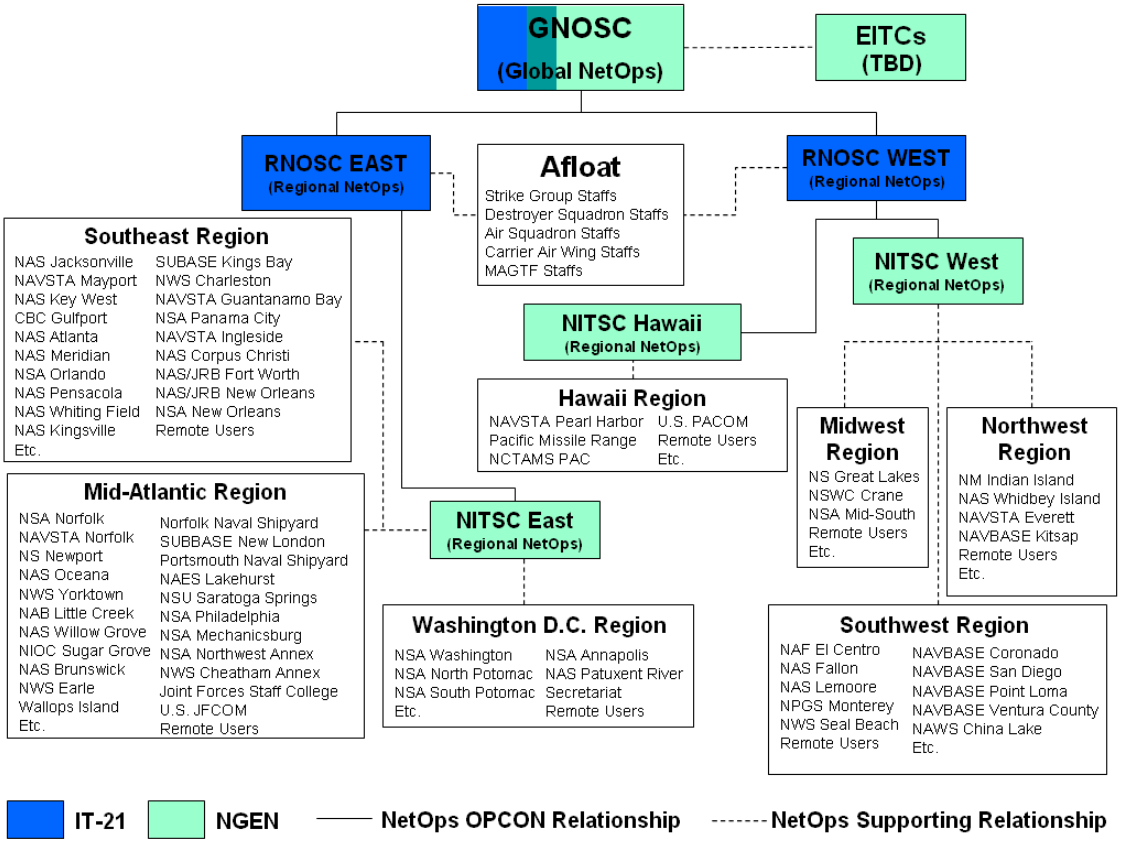


Figure 5 summarizes the OPCON relationships between the unified combatant commands and Navy component commands as well as the supporting NetOps relationships between Navy

commands and the appropriate regional NetOps authority. Figure 6 summarizes the headquarters of the supporting establishment and the supporting NetOps relationships with regional NetOps authorities.

Figure 5: Regional USN C2 and NetOps C2 Relationships

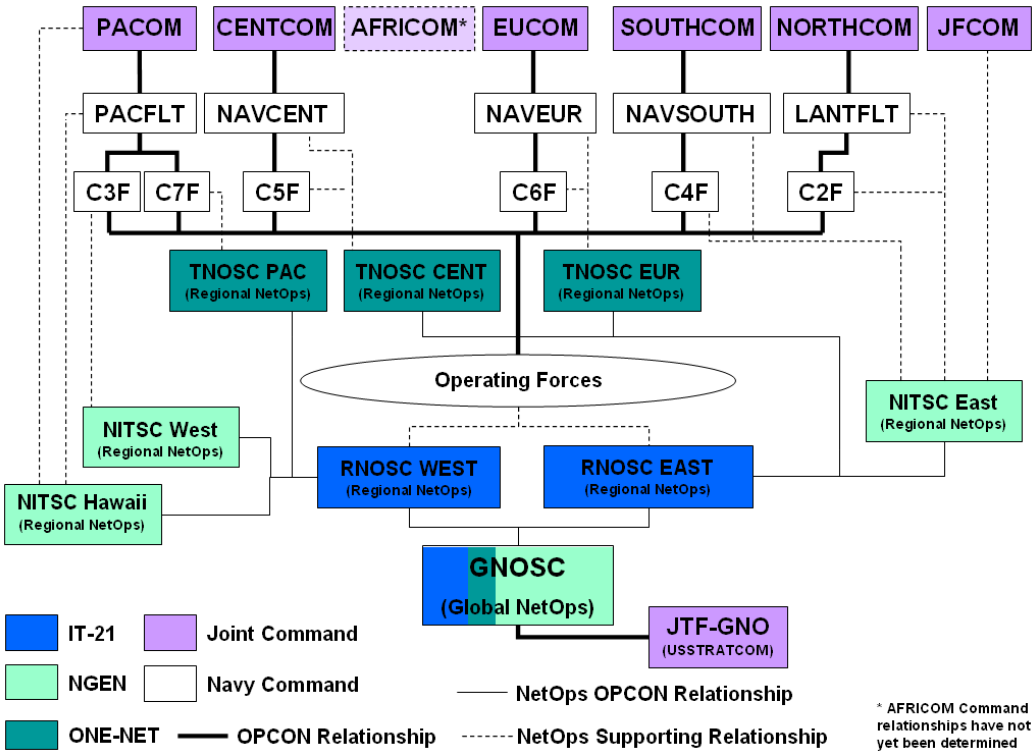
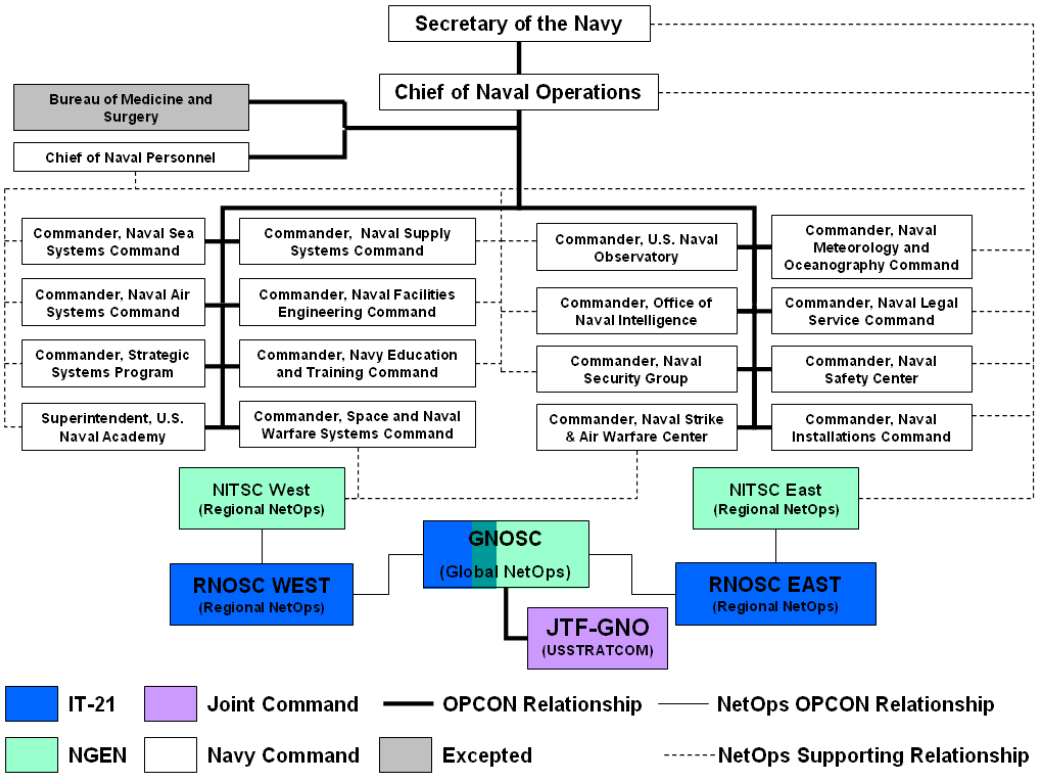


Figure 6: USN Supporting Establishment and NetOps Supporting Relationships



4.4 USMC NGEN Management Domain

This section describes the global, regional, and local NetOps authorities responsible for the operation and defense of the USMC NGEN MD.

4.4.1 Global NetOps

MCNOSC shall operate the GNOSC for the USMC NGEN MD and exert global NetOps OPCON over it. MCNOSC directs global network operations and network defense of the MCEN and provides technical leadership to facilitate seamless information exchange in support of Marine forces operating worldwide. The USMC GNOSC will have the following NGEN responsibilities:

- **Shifting supporting responsibilities when necessary**. The GNOSC is responsible for re-assigning support relationships. For example, the GNOSC could re-assign supporting responsibilities when operational forces deploy from one region to another or in response to operational/network events.
- **Providing authoritative direction needed to coordinate global operations**. Certain management functions, such as security, need to occur on a global scale. The GNOSC shall provide the authoritative direction needed for services that require global management.
- **Assigning tasks and objectives in response to global network events**. The GNOSC shall establish global priorities and assign tasks and objectives to subordinates to accomplish them.

USMC EITCs are data centers that will host enterprise-class applications/services required by the supporting establishment and the warfighter. USMC EITCs will be subordinate to the USMC GNOSC, who is responsible for directing and coordinating global functions.

4.4.2 Regional NetOps

Each RNOSC will take NetOps direction from the GNOSC through Commander MCNOSC's NetOps OPCON authority, and shall exert regional NetOps OPCON over its assigned segment of the USMC NGEN MD by:

- **Responding to direction and tasking from the USMC GNOSC**. The USMC GNOSC maintains global NetOps OPCON over the USMC MD.
- **Providing authoritative direction needed to coordinate regional operations**. The RNOSC shall provide the authoritative direction needed for regional management functions.
- **Assigning tasks and objectives in response to regional network events**. The RNOSC shall establish regional priorities and assign tasks and objectives to subordinates to accomplish them.
- **Managing IT resources and services for supported commands and users**. The RNOSC is responsible for managing its IT resources and services on behalf of the commands/users it is responsible for supporting.

The RNOSC, generally established at the Marine Corps Bases Command level to support Marine Forces (MARFOR) Commands, shall delegate NetOps authorities to MITSCs to provide regional NetOps capabilities. Each MITSC will host services and applications and support forces as designated by Director C4. MITSCs are generally provisioned within a Marine Corps Installation (MCI) Commands to support Marine Expeditionary Force (MEF) Commands and, as part of the fifth element of the MAGTF, support the warfighter while operationally deployed, in garrison, or engaged in training.

4.4.3 Local NetOps

Base G6s will act as the local NetOps authority and shall exert NetOps TACON over their designated area of responsibility by:

- **Responding to direction and tasking from the GNOSC, RNOSCs, and MITSCs**. The local NetOps authority shall respond to tasking and direction from higher NetOps authorities.
- **Managing access control for supported commands**. The local NetOps authority shall support the management of access to NGEN.
- **Managing all locally hosted services and applications**. Some services and applications might be hosted and/or managed by the local NetOps authority.

Deployed MAGTFs will constitute their own MD and have local NetOps authority when deployed in support of military operations or engaged in training exercises. When deployed as

part of a Joint or Multinational force, operational tasking and reporting for these commands will occur as established by their Joint or Multinational command authority.

4.4.4 Summary of the USMC MD

The NetOps C2 relationships outlined in this section strikes a balance between the need for global end-to-end management and the operational flexibility of regionally or locally delivered support. The GNOSC delegates some NetOps authority to the RNOSCs, who then delegate some authority to MITSCs, to support regional NetOps capabilities that are more responsive to the needs of operating forces. The global and regional NetOps authorities also delegate some NetOps authority to Base G6s to support local NetOps capabilities that are more responsive to the needs of individual commands. The intent of this NetOps C2 structure is to delegate appropriate authorities to regional and local NetOps authorities to improve responsiveness and flexibility within the MD while not jeopardizing global operations and priorities. Figure 7 summarizes the global, regional, and local NetOps C2 relationships for the USMC NGEN MD. Figure 8 summarizes the OPCON relationships between the unified combatant commands and USMC component commands as well as the supporting NetOps relationships between USMC commands and the appropriate regional NetOps authority.

Figure 7: NetOps C2 Relationships for the USMC NGEN Management Domain

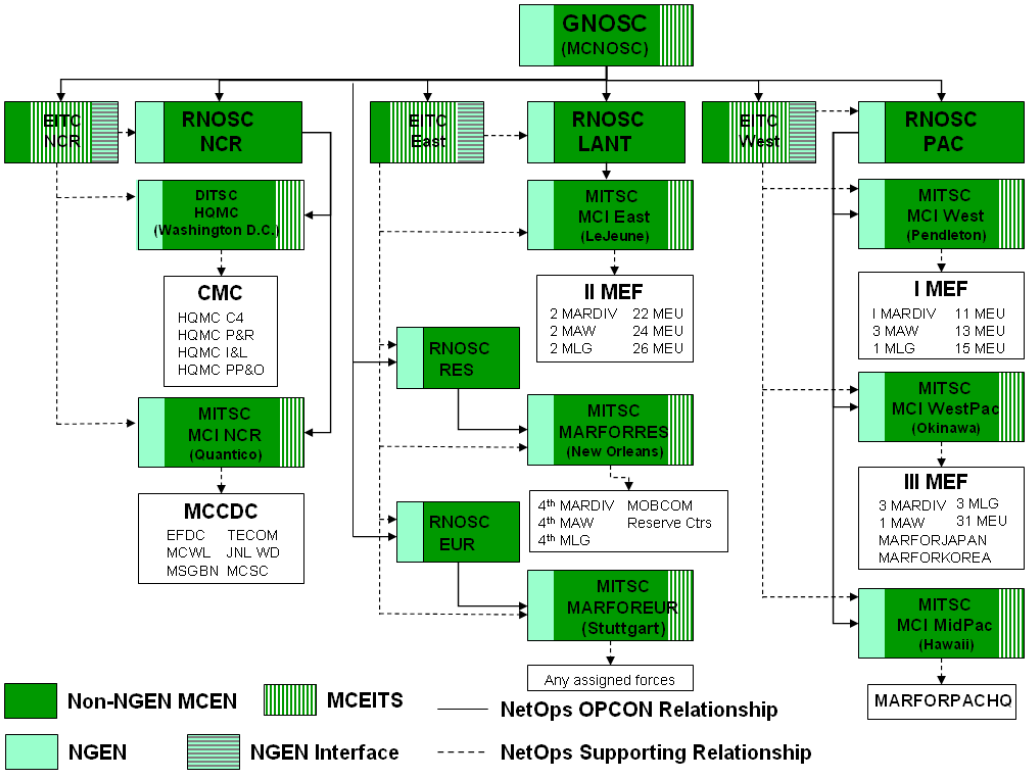
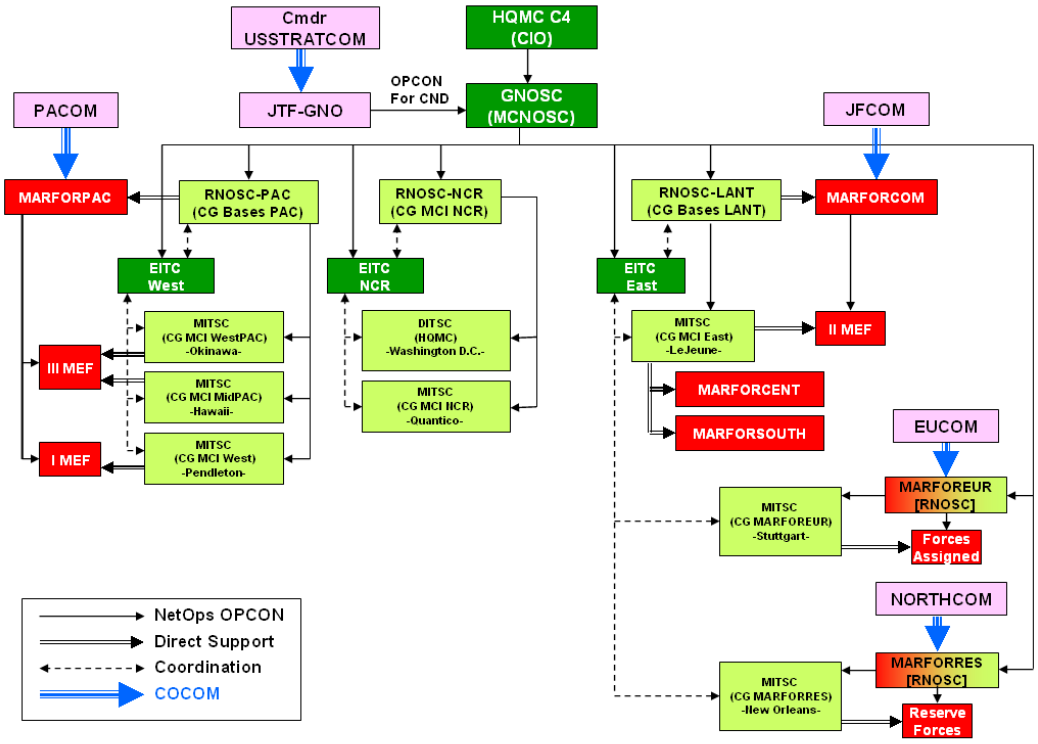


Figure 8: Regional USMC C2 and NetOps C2 Relationships



4.5 Relationship between NGEN Management Domains

The USN and USMC GNOSCs need to exchange information on the status of their respective MDs, work together to address NGEN problems, and conduct collaborative planning to address current as well as future security threats. As outlined in Section 3, several NGEN requirements necessary to ensure the coordination of NetOps activities across the USN and USMC NGEN MDs are:

- **Common set of reporting, planning, and execution tools for the vendor and the DON**. A common set of tools and interfaces are needed to coordinate EM, ND, and CM NetOps mission essential tasks across the two NGEN MDs.
- **Ability to create, maintain, and display consistent operational pictures of the status of NGEN**. Consistent operational pictures are needed for reporting the status, threat, vulnerability, and mission impact of degradation for each NGEN MD in a manner which can be tailored to the interests of the other MDs.
- **Interoperable trouble ticket management system for the vendor and the DON**. Both NGEN MDs need to use an interoperable trouble ticket system to track NGEN trouble tickets.

4.6 Relationship with the Joint Task Force – Global Network Operations

The JTF-GNO directs the operation and defense of the GIG. The Unified Command Plan, dated March 2005, assigned Commander, USSTRATCOM as the Combatant Commander for

Information Operations and Global C4ISR. The Secretary of Defense signed a delegation of authority letter on 18 June 2004, designating the Director, DISA as the Deputy Commander for GNO and the new Commander of the JTF-GNO.

As specified in the Forces For Unified Commands Memorandum, dated 15 February 2006, JTF-GNO has OPCON over DOD NetOps organizations and Service NetOps Components. JTF-GNO will also exercise TACON over the Service computer emergency response teams (CERTs) and computer incident response teams (CIRTs).[2] As outlined in Section 3, several NGEN requirements necessary to support these OPCON and TACON relationships between JTF-GNO and NGEN GNOSCs are:

- **Ability to create, maintain, and display consistent operational pictures of the status of NGEN**. NGEN needs to provide situational awareness of its own problems and threats that might impact the GIG to allow Joint NetOps authorities to take proactive measures and minimize global impact. Consistent operational pictures are needed for reporting status, threat, vulnerability, and mission impact of degradation to JTF-GNO and Commanders in a manner tailored to its areas of responsibility/interest.

- **Common set of reporting and planning tools for the DON and JTF-GNO**. NGEN NetOps authorities need to work closely with their counterparts at JTF-GNO to keep them apprised of the status of NGEN and collaboratively develop courses of action in response to current or emerging NetOps threats.
- **Ability to obtain and display information from JTF-GNO**. NGEN needs visibility into the status of the GIG, its current threat environment, etc. to provide situational awareness into problems or threats that might impact NGEN and allow its NetOps commanders to take proactive measures to address them.

In addition to the ability to share information and collaborate in near-real time with JTF-GNO (as outlined above), the USN and USMC GNOSCs must also support the incident reporting structure outlined in CJCSM 6510.01.

---

[2] In the case of the USMC, CERT capabilities are incorporated into the MCNOSC and a separate TACON authority over these capabilities is not exercised by JTF-GNO. Instead, JTF-GNO exercises OPCON for ND over the MCNOSC because the Commanding Officer, MCNOSC is the single USMC command authority for both GNOSC and CERT capabilities.

5 NGEN Services and NetOps

5.1 End-User Computing Services

Table 1 contains a representative list of NGEN end-user computing services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 1: NetOps Responsibilities for End-User Computing Services

End User Computing Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
LAN	**NetOps OPCON** Establish regional authorities and responsibilities	**NetOps OPCON** Manage LAN infrastructure Designate local responsibilities	**NetOps TACON** Support LAN installation and maintenance Execute Move/Add/Change	Designate seat locations Provide physical security for LAN Provide command LAN requirements
Seat	**NetOps OPCON** Monitor seat utilization and ensure enterprise capabilities to support seats	**NetOps OPCON** Manage seat resources	**NetOps TACON** Support seat installation and maintenance Execute Move/Add/Change	Provide physical security for seats Provide command seat requirements
Scan/Print /Fax	**NetOps OPCON** Monitor scanner/printer/fax utilization and ensure enterprise capabilities to support scanners/printers/ faxes	**NetOps OPCON** Manage scanner/printer/fax resources	**NetOps TACON** Support scanner/printer/fax installation and maintenance Execute Move/Add/Change	Provide physical security for scanners, printers, and faxes Provide command scanner, printer, and fax requirements
Remote Access	**NetOps OPCON** Establish regional authorities and responsibilities Monitor gateways for remote access	**NetOps OPCON** Manage gateways for remote access		Provide command remote access requirements
Account	**NetOps OPCON** Establish regional authorities and responsibilities Ensure enterprise capabilities to manage accounts and associated permissions/access control	**NetOps OPCON** Manage regional accounts, permissions and access controls Designate local responsibilities	**NetOps TACON** Validate requests for accounts and permissions Monitor access and use	Provide command requirements for accounts and access or revoking access

5.2 Network Services

Table 2 contains a representative list of NGEN network services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 2: NetOps Responsibilities for Network Services

Network Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
WAN	**NetOps OPCON** Manage WAN infrastructure Supports WAN installation and maintenance	Provide regional WAN requirements		
BAN	**NetOps OPCON** Establishes regional authorities and responsibilities	**NetOps OPCON** Manage BAN infrastructure Designate local responsibilities	**NetOps TACON** Support BAN installation and maintenance Provide BAN requirements	
Video Teleconferencing (VTC)	**NetOps OPCON** Establish regional authorities and responsibilities	**NetOps OPCON** Manage regional VTC bridges Designate local responsibilities	**NetOps TACON** Support VTC installation and maintenance	Operate VTC in accordance with established guidance Provide physical security of VTC equipment Provide command VTC requirements

5.3 Application Management Services

Table 3 contains a representative list of NGEN application management services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 3: NetOps Responsibilities for Application Management Services

Application Management Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
E-mail	**NetOps OPCON** Manage global address list Establish regional authorities and responsibilities Apportion e-mail resources to regional authorities	**NetOps OPCON** Manage regional e-mail resources Designate local responsibilities	**NetOps TACON** Manage user mailboxes, permissions, and functional accounts for supported commands	Provide command e-mail requirements Determine user mailbox sizes, permissions, and functional accounts of the command within the limits established by the regional authority
File Storage	**NetOps OPCON** Establish file storage resources for region	**NetOps OPCON** Manage file storage resources in the region Designate local responsibilities		Provide command file storage requirements **NetOps TACON** Manage access rights, file shares, and folders in accordance with established guidance
Defense Messaging System (DMS)	**NetOps OPCON** Function as DMS COC by directing Service DMS operations and managing X.500 directory Establish regional authorities and responsibilities	**NetOps OPCON** Manage regional DMS gateways Designate local responsibilities	**NetOps TACON** Adds/removes users from DMS list for supported commands	Validate access to command messages
Desktop	**NetOps OPCON** Approve gold disk applications Approve regional desktop requirements	Provide regional desktop requirements		Provide command desktop requirements
Application Installation and Removal	**NetOps OPCON** Authorize and direct installations, upgrades or removal for MD Establish regional authorities and responsibilities	**NetOps OPCON** Support remote installation, upgrade or removal Designate local responsibilities	**NetOps TACON** Support manual installation, upgrade or removal for supported commands, as assigned, when global/regional capabilities fail in time critical situations	Support manual installation, upgrade or removal when directed

5.4 Data Center Services

Table 4 contains a representative list of NGEN midrange services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 4: NetOps Responsibilities for Data Center Services

Data Center Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
Server Hosting	**NetOps OPCON** Manage Enterprise IT Centers and regional enterprise platforms	**NetOps OPCON** Manage regional centers and services Support the plug-and-play of tactical systems as required		**NetOps TACON** Manage tactical resources in accordance with established guidance
Back-Up	**NetOps OPCON** Manage data back-up operations for global services	**NetOps OPCON** Manage data back-up operations for regional and local services Approve regional back-up requirements		Provide command back-up requirements Designate and stage data for back-up service
COOP/DR	**NetOps OPCON** Manage COOP/DR service between regions	**NetOps OPCON** Manage COOP/DR service within region Designate local responsibilities	**NetOps TACON** Execute COOP/DR in accordance with established guidance	Provide command COOP/DR requirements
Facility	**NetOps OPCON** Coordinate facility maintenance and upkeep with global provider(s)	**NetOps OPCON** Coordinate facility maintenance and upkeep with regional provider(s)		

5.5 Service Desk Services

Table 5 contains a representative list of NGEN service desk services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 5: NetOps Responsibilities for Service Desk Services

Service Desk Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
Trouble Ticket System	**NetOps OPCON** Manages trouble ticket system Responds to global issues	**NetOps OPCON** Responds to regional issues	**NetOps TACON** Responds to local issues	Visibility into the command's open trouble tickets

5.6 Security Services

Table 6 contains a representative list of NGEN security services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 6: NetOps Responsibilities for Security Services

Security Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
Public Key Infrastructure (PKI)	**NetOps OPCON** Manages the PKI service Designate regional responsibilities	**NetOps OPCON** Manages security groups Designate local responsibilities	**NetOps TACON** Add/remove users from the exception list	
Boundary Security and DMZs	**NetOps OPCON** Manages all B1 and B2 boundaries Designate COOP/DR responsibilities	**NetOps OPCON** Manages designated B1 and B2 boundaries in specified COOP/DR situations		
Classified Spill Cleanup	**NetOps OPCON** Manages spill cleanup on enterprise-class services Directs spill cleanup by regional and/or local authorities	**NetOps OPCON** Manages spill cleanup on regional services Directs spill cleanup by local authorities	**NetOps TACON** Manages spill cleanup on local seats and services	Report spills and support spill cleanup on local seats and services
Anti-Virus	**NetOps OPCON** Manages anti-virus service Directs anti-virus scanning by regional and/or local authorities	**NetOps OPCON** Supports anti-virus scan/removal on regional services Designates local responsibilities	**NetOps TACON** Supports anti-virus scan/removal on local services and seats	Support the prevention and identification of viruses
Anti-Spyware	**NetOps OPCON** Manages anti-spyware service Directs anti-spyware scanning by regional and/or local authorities	**NetOps OPCON** Supports anti-spyware scan/blocking on regional services Designates local responsibilities	**NetOps TACON** Supports anti-spyware scan/removal on local services and seats	Support the prevention and identification of spyware
Security Scanning and Monitoring	**NetOps OPCON** Monitor and analyze to detect unauthorized activity at global level Establishes regional authorities and responsibilities	**NetOps OPCON** Monitor and analyze to detect unauthorized activity at regional level Designates local responsibilities	**NetOps TACON** Support efforts to detect and correct unauthorized activity	Support the prevention and identification of unauthorized activity Assess operational impact of security events
Anti-Spam	**NetOps OPCON** Manages anti-spam service Establishes regional authorities and responsibilities	**NetOps OPCON** Approve additions/removal from regional spam filter		Identify Spam

5.7 Service Coordination

Table 7 contains a representative list of NGEN service coordination services and the types of NetOps controls/functions at the global, regional, and local levels for each service.

Table 7: NetOps Responsibilities for Service Coordination Services

Service Coordination Services	Global NetOps	Regional NetOps	Local NetOps	
	GNOSC	*RNOSC/ITSC*	*USN Detachment USMC Base G6*	*Command*
Configuration Management	**NetOps OPCON** Update configuration management database Audit configurations for compliance Designate regional and local responsibilities	**NetOps OPCON** Update configuration management database Audit regional configurations and report level of compliance	**NetOps TACON** Update configuration management database Audit local configurations and report level of compliance	
Performance Monitoring	**NetOps OPCON** Monitor performance of global services	**NetOps OPCON** Monitor performance of regional and local services		Identify unacceptable performance

6 IT Service Management

This section defines IT Service Management (ITSM) within the IT Infrastructure Library (ITIL) and uses definitions from the ITIL publications for *Service Strategy, Service Design, Service Transition, Service Operation,* and *Continual Service Improvement*[3].

6.1 IT Service Management

ITSM is a discipline for managing IT systems that is philosophically centered on the user's perspective of IT's contribution to operations. ITSM is not concerned with the details of how to use a particular vendor's product or with the technical details of the systems under management. Instead, ITSM focuses on providing a framework to structure IT-related activities and the interactions of IT technical personnel with users. ITSM will be the framework through which NGEN NetOps will be achieved.

6.2 Information Technology Infrastructure Library

ITIL is a set of concepts and techniques for managing the development and operation of IT infrastructure. ITIL is published in a series of books, each of which cover an IT-management topic, which provide a detailed description of important IT practices with comprehensive checklists, tasks, and procedures. The advantage of describing ITSM within an ITIL framework is all of the ITIL processes, functions, and terminology are clearly defined and industry is well versed with the ITIL framework.

The most recent version of ITIL (version 3) consists of five publications that examine the entire lifecycle of an IT service:

- **Service Strategy**. Provides guidance on how to design, develop, and implement IT services. Financial management, demand management, and service portfolio management are among other major topics discussed in the *Service Strategy* publication.
- **Service Design**. Provides guidance for the design and development of IT services. It covers design principles and methods for converting strategic objectives into portfolios of services and service assets. Service catalogue management, service level management, capacity management, availability management, IT service continuity management, information security management, and supplier management are topics discussed in the *Service Design* publication.
- **Service Transition**. Provides guidance for transitioning both new services and changes to existing services into operations. Change management, configuration management, and release management are topics discussed in the *Service Transition* publication.

[3] The five ITIL (version 3) publications were developed by the U.K.'s Office of Government Commerce (OGC) and published by The Stationary Office (TSO) on 30 May 2007.

- **Service Operation**. Provides guidance on effective and efficient delivery and support of services to ensure value for the customer. Event management, incident management, service desk operations, problem management, and access management are topics discussed in the *Service Operation* publication.
- **Service Improvement**. Aspects of service level management that address reviewing and improving service performance are discussed in the *Service Improvement* publication.

6.3 Achieving NetOps via ITSM/ITIL

Table 8 maps ITSM/ITIL management processes to NetOps mission essential tasks. The advantage of mapping the NetOps mission essential tasks into an ITIL framework is the ITIL processes, functions, and terminology are clearly defined and provides a common lexicon to describe NetOps processes and functions.

Table 8: Relating ITSM/ITIL Management Practices with NetOps Mission Essential Tasks

ITIL Function	**NetOps Mission Essential Tasks**		
	Enterprise Mgmt	*Network Defense*	*Content Mgmt*
Service Strategy ▪ Financial Mgmt ▪ Demand Mgmt ▪ Service Portfolio Mgmt	✓ Develop a EM strategy	✓ Develop a ND strategy	✓ Develop a CM strategy
Service Design ▪ Service Catalogue Mgmt ▪ Service Level Mgmt ▪ Capacity Mgmt ▪ Availability Mgmt ▪ IT Service Continuity Mgmt ▪ Information Security Mgmt ▪ Supplier Mgmt	✓ Ensure the EM strategy is reflected in the design of services	✓ Ensure the ND strategy is reflected in the design of services	✓ Ensure CM strategy is reflected in the design of services
Service Transition ▪ Change Mgmt ▪ Configuration Mgmt ▪ Release Mgmt	✓ Ensure seamless transition of EM services	✓ Ensure service transitions occur in a secure manner	✓ Ensure seamless transition of CM services
Service Operation ▪ Event Mgmt ▪ Incident Mgmt ▪ Service Desk ▪ Problem Mgmt ▪ Access Mgmt	✓ Support daily operations and respond to network events/incidents/problems	✓ Support daily ND operations and respond to security events/incidents/problems	✓ Ensure content is available to the right user at the right time and in the right location
Service Improvement ▪ Service Level Mgmt	✓ Change EM features within services in response to changes in operational requirements	✓ Change ND features in services in response to changes in the threat environment and risk to operations	✓ Change CM features within services in response to changes in user or operational requirements

6.4 Implementing ITSM on NGEN

Sections 7 through 11, with supporting annexes, outline how the ITIL management functions associated with service strategy, design, transition, operation, and improvement – respectively – can be implemented by NGEN. The emphasis of these sections will be on how NGEN NetOps will be achieved and supported using ITSM best practices. Each section contains the sub-sections that:

- **Define ITIL management functions**. The first sub-section provides a brief definition of relevant ITIL management functions.
- **Define NetOps management responsibilities**. All ITIL management functions will be performed, either entirely or in part, by organizations with governance, acquisition, and NetOps responsibilities:
  - *Governance*. The DON CIO, OPNAV N6 (as the Deputy DON CIO – Navy), and USMC C4 (as the Deputy DON CIO – USMC) provide overarching policies and directions for DON networks.
  - *Acquisition*. The Program Executive Office (PEO) for Enterprise Information Systems (EIS) is responsible for developing and procuring NGEN.
  - *NetOps*. The Commander, NETWARCOM is the Service component command authority for the Navy Enterprise Network. The Commander, MCNOSC is the Service Component Commander for the MCEN.

  The second sub-section highlights the NetOps responsibilities associated with each ITIL management function.
- **Determine level of DON authority over NetOps management activities**. The final sub-section outlines the level of contractor involvement, using the criteria outlined in Annex C, for each NetOps management activity. The following ratings, based on the criteria outlined in Annex C, will be used and color coded according to their level of risk, which increases with the level of contractor involvement:
  - *G1 (green)*. The activity is a management control function that is inherently a DON function and cannot be outsourced. There is a subtle difference between the DON exerting management control over NGEN and the actual execution. For example, a contractor can develop a capacity plan. DON exerts management control by approving (or rejecting) the plan. A contractor, who could be the same one or a different one, can be responsible for executing the plan.
  - *To Be Determined (TBD)*. The activity could be a critical function, require a DON capability to mitigate operational risk or require a DON competency to support training and retention.
  - *G5 (red)*. The activity can be completely outsourced.

Annexes D through U outline the ITILv3 management process and provides use cases to illustrate its application to NGEN NetOps. The ITILv3 processes depicted in the Annexes provide a starting point for further development and refinement as NGEN is procured and fielded.

7 NGEN Service Strategy

This section uses information from the *Service Strategy* publication, the functional responsibility decision criteria (FRDC) summarized in Annex C, and the service strategy processes for NGEN outlined in Annexes D through F to determine NetOps responsibilities and level of DON authority over service strategy functions.

7.1 ITIL Service Strategy Functions

The ITIL management processes for service strategy development are:

- **Financial Management**. Assesses the overall value of an IT service, the costs of the underlying assets associated with its provisioning, and its impact on operations. [Annex D contains a more detailed discussion of financial management]
- **Demand Management**. Assess the expected usage levels of the service and cost saving options (e.g., off-peak pricing, volume discounts, differentiated service, etc.). [Annex E contains a more detailed discussion of demand management]
- **Service Portfolio Management**. Process by which investments in different services across the enterprise are made to maximize the overall return on investment. [Annex F contains a more detailed discussion of service portfolio management]

7.2 NGEN Service Strategy

Table 9 summarizes the governance, acquisition, and NetOps responsibilities for the development of service strategies.

Table 9: Governance, Acquisition, and NetOps Responsibilities for Service Strategy

ITIL Management Function	Governance (DON CIO, OPNAV N6, and USMC C4)	Acquisition (PEO EIS)	NetOps (NETWARCOM and MCNOSC)
Financial Management	✓ Ensure compliance with agreed upon accounting methods and practices	✓ Provide service valuation, accounting, and tracking of service expenses	✓ Provide operational data on service usage
Demand Management		✓ Perform demand modeling and develop service options for estimated demand	✓ Provide usage data
Service Portfolio Management	✓ Establish service priorities and authorize resources	✓ Inventory services; validate portfolio data; provide cost/ROI data; and charter services	✓ Provide operational prioritization of services

7.3 NetOps Service Strategy Authority

Table 10 combines the FRDC summarized in Annex C with the processes outlined in Annexes D through F to determine the level of DON authority over different NetOps management functions related to service strategy.

Table 10: Level of DON NetOps Authority over Service Strategy Functions

Service Strategy Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Financial Management			
Perform trend analysis			
Gather cost data			
Develop IT budgets			
Review bills from suppliers			
Approve charges			
Certify Charges			
Create financial reports			
Approve IT budgets			
Conduct periodic audits			
Assess financial management framework			
Change framework			
Develop financial management framework			
Approve financial management framework			
Assign responsibilities to organizations			
Demand Management			
Perform service modeling			
Perform capacity modeling			
Validate modeling results			
Assess service demand			
Develop service demand model			
Approve service demand model			
Service Portfolio Management			
Develop service options			
Develop cost models			
Determine best service option			
Approve service options			
Approve service			
Prioritize services			
Approve service prioritization			
Develop service portfolio management framework			
Approve service portfolio management framework			
Assign responsibilities to organizations			
Assess service portfolio management framework			

G1	**The activity is a management control function and cannot be outsourced.**
TBD	**To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**
G5	**The activity can be completely outsourced.**
	No NetOps responsibilities.

8 NGEN Service Design

This section uses information from the *Service Design* publication, the FRDC summarized in Annex C, and the service design processes for NGEN outlined in Annexes G through M to determine NetOps responsibilities and level of DON authority over service design functions.

8.1 ITIL Service Design

The ITIL management processes for service design and development are:

- **Service Catalogue Management**. Provides a single source of consistent information on all of the agreed services that is widely available to those who are approved to access it. [Annex G contains a more detailed discussion of service catalogue management]
- **Service Level Management**. Determines appropriate IT service targets, ensures an agreed level of service is provided for all current IT services, and future services are delivered to agreed targets. [Annex H contains a more detailed discussion of service level management]
- **Capacity Management**. Includes capacity planning activities and assisting with the diagnosis of capacity-related problems. [Annex I contains a more detailed discussion of capacity management]
- **Availability Management**. Ensures the level of service availability delivered in all services either meets or exceeds current and/or future operational requirements. [Annex J contains a more detailed discussion of availability management]
- **IT Service Continuity Management**. Ensures required IT services can be resumed within the timescales required to support operations. [Annex K contains a more detailed discussion of IT service continuity management]
- **Information Security Management**. Align IT security with DoD IA program requirements and operational requirements/objectives to ensure the security of the network, its services, and its applications. [Annex L contains a more detailed discussion of information security management]
- **Supplier Management**. Processes by which suppliers are managed to provide quality IT services in support of operations, and to ensure these services are provided at reasonable costs. [Annex M contains a more detailed discussion of supplier management]

8.2 NGEN Service Design

Table 11 summarizes the governance, acquisition, and NetOps responsibilities for the development and design of services.

Table 11: Governance, Acquisition, and NetOps Responsibilities for Service Design

ITIL Management Function	Governance (DON CIO, OPNAV N6, and USMC C4)	Acquisition (PEO EIS)	NetOps (NETWARCOM and MCNOSC)
Service Catalogue Management		✓ Define services and develop/maintain service catalogue	✓ Provide operational requirements
Service Level Management	✓ Establish service level mgmt framework	✓ Develop SLAs/OLAs and determine SLA/OLA breaches	✓ Provide service requirements and perform service monitor/reporting
Capacity Management	✓ Establish capacity mgmt framework	✓ Perform service/capacity modeling; predict future usage; and develop/ maintain up-to-date capacity plan	✓ Perform trend analysis; approve capacity plan; and develop mitigation plans
Availability Management	✓ Establish availability mgmt framework	✓ Develop availability targets, design criteria, and plans	✓ Investigate availability issues and develop mitigation plans
IT Service Continuity Management	✓ Establish IT service continuity mgmt framework	✓ Perform impact/risk analysis and develop service continuity plan	✓ Provide operational inputs to risk analysis and test service continuity plan
Information Security Management	✓ Produce, maintain, distribute, and enforce IA/IT security policies	✓ Implement security controls in services; and proactively improve security controls	✓ Comply with IA/IT security policies; monitor for and respond to unauthorized activity; document breaches/incidents; and comply with JTF-GNO direction
Supplier Management		✓ Manage supplier relationships and negotiate contracts	

8.3 NetOps Service Design Authority

Table 12 combines the FRDC summarized in Annex C with the processes outlined in Annexes G through M to determine the level of DON authority over different NetOps management functions related to service design.

Table 12: Level of DON NetOps Authority over Service Design Functions

Service Design Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Service Catalogue Management			
Develop service definitions			
Approve service definitions			
Develop and maintain service catalogue			
Service Level Management			
Develop service requirements	TBD	TBD	
Approve service requirements	G1	G1	
Monitor and assess performance	G1	G1	
Review service requirements	TBD	TBD	
Modify service or operational level agreement?	G1	G1	
Develop service level agreements (SLAs)			
Develop operational level agreements (OLAs)			
Approve SLAs and OLAs			
Breach of SLAs and OLAs			
Develop service level management framework			
Approve framework			
Assign service level management responsibilities			
Analyze SLA/OLA breaches			
Assess framework			
Change framework?			
Capacity Management			
Perform trend analysis	TBD	TBD	
Approve capacity plan	G1	G1	
Develop mitigation plan	TBD	TBD	
Approve mitigation plan	G1	G1	
Disseminate mitigation plan	TBD	TBD	
Perform service modeling			
Perform capacity modeling			
Predict future capacity usage			
Develop capacity plan			
Develop capacity management framework			
Approve framework			
Assign capacity management responsibilities			
Analyze capacity problems			
Assess framework			
Change framework?			

G1	**The activity is a management control function and cannot be outsourced.**
TBD	**To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**
G5	**The activity can be completely outsourced.**
	No NetOps responsibilities.

Table 12: Level of DON NetOps Authority over Service Design Functions (Cont.)

Service Design Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Availability Management			
Investigate availability issues	TBD	TBD	
Develop mitigation plan	TBD	TBD	
Approve mitigation plan	G1	G1	
Disseminate mitigation plan	TBD	TBD	
Determine availability targets			
Determine availability design criteria			
Develop availability plan			
Approve availability plan			
Develop availability management framework			
Approve framework			
Assign availability management responsibilities			
Analyze availability problems			
Assess framework			
Change framework?			
IT Service Continuity Management			
Develop service continuity requirements	TBD	TBD	
Approve service continuity requirements	G1	G1	
Develop procedures for continuity plan	TBD	TBD	
Approve procedures for continuity plan	G1	G1	
Periodic continuity training/exercise	TBD	TBD	
Execute continuity plan	G1	G1	
Develop service continuity plan			
Approve service continuity plan			
Information Security Management			
Are new controls required?	G1	G1	
Perform penetration testing/audits	TBD	TBD	
Analyze emerging security threats	TBD	TBD	
Analyze security breaches and incidents	TBD	TBD	
Report security vulnerabilities	TBD	TBD	
Review IA/CND/CIP policies	TBD	TBD	
Are changes to the policies required?	G1	G1	
Approve security controls	G1	G1	
Develop IA/CND/CIP policies			
Approve policies			
Disseminate policies			
Develop new security controls			
Supplier Management			
Develop contract			
Approve contract			
Conduct source selection			
Approve source selection			
Monitor contract performance			
Change contract?			
Renew contract?			
Terminate contract?			
Modify contract			
Approve contract modification			

G1	**The activity is a management control function and cannot be outsourced.**
TBD	**To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**
G5	**The activity can be completely outsourced.**
	No NetOps responsibilities.

9 NGEN Service Transition

This section uses information from the *Service Transition* publication, the FRDC summarized in Annex C, and the service transition processes for NGEN outlined in Annexes N through P to determine NetOps responsibilities and level of DON authority over service transition functions.

9.1 ITIL Service Transition

The ITIL management processes that support the transition to a service are:

- **Change Management**. Processes that ensure changes are evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. [Annex N contains a more detailed discussion of change management]
- **Release Management**. Processes that deploy both new services and changes to existing services into the enterprise and establish effective use of these services in support of operations. [Annex O contains a more detailed discussion of release management]
- **Configuration Management**. Processes that document and control the components of IT services and maintain accurate information on the historical, current, and planned state of these services and their underlying components. [Annex P contains a more detailed discussion of configuration management]

9.2 NGEN Service Transition

Table 13 summarizes the governance, acquisition, and NetOps responsibilities for service transition.

Table 13: Governance, Acquisition, and NetOps Responsibilities for Service Transition

ITIL Management Function	Governance (DON CIO, OPNAV N6, and USMC C4)	Acquisition (PEO EIS)	NetOps (NETWARCOM and MCNOSC)
Change Management	✓ Establish change mgmt framework; assess whether changes comply with DON standards; and approve scope of the changes	✓ Evaluate change requests; develop implementation plan; comply with DIACAP for changes that affect the security posture of the network; and approve changes	✓ Generate Requests for Change (RFCs) from operational forces; validate RFCs; and authorize changes
Release Management	✓ Establish release mgmt framework	✓ Develop roll-out/back-out plans; distribute release; provide training; and conduct operational testing	✓ Approve roll-out/back-out plans; and accept release
Configuration Management	✓ Establish configuration mgmt framework	✓ Maintain a NGEN Configuration Management Database with historical, current, and planned configurations	✓ Implement standard configuration changes; update Configuration Management Database; and monitor configuration status

9.3 NetOps Service Transition Authority

Table 14 combines the DON FRDC summarized in Annex C with the processes outlined in Annexes N through P to determine the level of DON authority over different NetOps management functions related to service transition.

Table 14: Level of DON NetOps Authority over Service Transition Functions

Service Transition Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Change Management			
Generate Request for Change (RFC)	TBD	TBD	TBD
Validate RFC	G1	G1	G1
Categorize & Classify RFC	TBD	TBD	
Authorize standard change	G1	G1	
Authorize change	G1		
Coordinate change	TBD		
Notify originator	G5		
Develop implementation plan			
Compliance with DON standards			
Approve waiver			
Approve DON-wide change			
Approve change for management domain			
Require C&A			
Perform C&A			
Approve change			
Require developmental testing			
Conduct developmental testing			
Evaluate testing			
Release Management			
Approve roll-out plan	G1	G1	
Approve back-out plan	G1	G1	
Accept release	G1	G1	
Develop release plan			
Approve release plan			
Build and configure release			
Develop roll-out plan			
Develop back-out plan			
Distribute release			
Conduct operational testing			
Conduct training			
Update architecture products			
Update configuration database			
Execute back-out plan			
Develop release mgmt framework			
Approve release mgmt framework			
Assign responsibilities			
Conduct periodic audits of releases			
Assess release mgmt framework			
Change release mgmt framework			

G1	**The activity is a management control function and cannot be outsourced.**
TBD	**To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**
G5	**The activity can be completely outsourced.**
	No NetOps responsibilities.

Table 14: Level of DON NetOps Authority over Service Transition Functions (Cont.)

Service Transition Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Configuration Management			
Recommend configuration items	TBD	TBD	
Approve configuration change	G1	G1	
Implement standard configuration change	TBD	TBD	
Update configuration database	TBD	TBD	
Extract configuration items from database	TBD	TBD	
Report configuration status	TBD	TBD	
Identify unauthorized configurations	TBD	TBD	
Develop configuration items			
Approve configuration items			
Develop configuration interfaces/controls			
Incorporate into configuration database			
Approve configuration controls			
Require change to service			
Implement configuration change			
Update architecture products			
Develop configuration mgmt framework			
Approve configuration mgmt framework			
Assign configuration mgmt responsibilities			
Assess configuration mgmt framework			
Change configuration mgmt framework			

G1	**The activity is a management control function and cannot be outsourced.**
TBD	**To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**
G5	**The activity can be completely outsourced.**
	No NetOps responsibilities.

10 NGEN Service Operation

This section uses information from the *Service Operation* publication, the FRDC summarized in Annex C, and the service operation processes for NGEN outlined in Annexes Q through U to determine NetOps responsibilities and level of DON authority over service operation functions.

10.1 ITIL Service Operation

The ITIL management processes that support the operation of a service are:

- **Event Management**. Processes to detect events[4], understand their underlying cause and/or impact, and determine the appropriate actions to either address or mitigate the event. [Annex Q contains a more detailed discussion of event management]
- **Incident Management**. Processes that restore normal service operation as quickly as possible and minimize the adverse impact on operations due to an incident[5]. [Annex R contains a more detailed discussion of incident management]
- **Problem Management**. Processes for identifying problems[6] and their root cause to drive changes to the service/infrastructure that will eliminate recurring incidents. [Annex S contains a more detailed discussion of problem management]
- **Service Desk**. Functional entity for addressing service requests and incident reports from users. Many of these service requests are typically small changes – low risk, frequently occurring, and low cost (e.g., a request to change a password, install an additional software application onto a particular workstation, and relocate desktop equipment). [Annex T contains a more detailed discussion of service desk operations]
- **Access Management**. Processes for granting authorized users the right to use a service, while preventing access to non-authorized users. NGEN users need single-user accounts that allow them to seamlessly move between MDs and roles. [Annex U contains a more detailed discussion of access management]

10.2 NGEN Service Operation

Table 15 summarizes the governance, acquisition, and NetOps responsibilities for service operation.

[4] An *event* is a change of state that is of significant importance to the management of an IT service.

[5] An *incident* is an unplanned interruption to or reduction in quality of an IT service.

[6] A *problem* is the cause of one or more incidents.

Table 15: Governance, Acquisition, and NetOps Responsibilities for Service Operation

ITIL Management Function	Governance (DON CIO, OPNAV N6, and USMC C4)	Acquisition (PEO EIS)	NetOps (NETWARCOM and MCNOSC)
Event Management			✓ Perform event identification, logging, and categorization; conduct event diagnosis; and take appropriate action
Incident Management			✓ Perform incident identification, logging, and categorization; conduct incident diagnosis; and take appropriate action
Problem Management		✓ Support problem detection, categorization, and diagnosis; and serve as a conduit to vendor support services	✓ Perform problem detection, logging, and categorization; conduct problem diagnosis; and take appropriate action
Service Desk			✓ Support the operations of a service desk; track open tickets; escalate requests when required; and close tickets after resolution
Access Management			✓ Verify identity; grant access privileges to services and data aligned with approved user access requirements and need to know; perform logging and tracking of service accesses; and remove or restrict access when appropriate

10.3 NetOps Service Operation Authority

Table 16 combines the FRDC summarized in Annex C with the processes outlined in Annexes Q through U to determine the level of DON authority over different NetOps management functions related to service operation.

Table 16: Level of DON NetOps Authority over Service Operation Functions

Service Operations Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Event Management			
Investigate & Diagnosis	TBD	TBD	TBD
Is it an event?	TBD	TBD	TBD
Is it an incident?	TBD	TBD	TBD
Is it a problem?	TBD	TBD	TBD
Develop event, incident and problem filters	TBD	TBD	TBD
Approve filters	G1	G1	G1
Is it a local, regional or global event?	TBD	TBD	TBD
Prioritize events	TBD	TBD	TBD
Approve prioritization of events	G1	G1	G1
Report event	TBD	TBD	TBD
Resolve event	TBD	TBD	TBD
Close event	TBD	TBD	TBD
Incident Management			
Investigate & Diagnosis	TBD	TBD	TBD
Is it an event?	TBD	TBD	TBD
Is it an incident?	TBD	TBD	TBD
Is it a problem?	TBD	TBD	TBD
Develop event, incident and problem filters	TBD	TBD	TBD
Approve filters	G1	G1	G1
Is it a local, regional or global incident?	TBD	TBD	TBD
Prioritize incidents	TBD	TBD	TBD
Approve prioritization of incidents	G1	G1	G1
Report incident	TBD	TBD	TBD
Resolve incident	TBD	TBD	TBD
Close incident	TBD	TBD	TBD
Problem Management			
Investigate & Diagnosis	TBD	TBD	TBD
Is it an event?	TBD	TBD	TBD
Is it an incident?	TBD	TBD	TBD
Is it a problem?	TBD	TBD	TBD
Develop event, incident and problem filters	TBD	TBD	TBD
Approve filters	G1	G1	G1
Is it a local, regional or global problem?	TBD	TBD	TBD
Prioritize problems	TBD	TBD	TBD
Approve prioritization of problems	G1	G1	G1
Generate Request for Change (RFC)	TBD	TBD	TBD

G1	The activity is a management control function and cannot be outsourced.
TBD	To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.
G5	The activity can be completely outsourced.
	No NetOps responsibilities.

Table 16: Level of DON NetOps Authority over Service Operation Functions (Cont.)

Service Operations Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Service Desk			
Open trouble ticket	G5	G5	
Provide Tier I technical support	TBD	TBD	
Is it an event?	TBD	TBD	
Is it an incident?	TBD	TBD	
Is it a problem?	TBD	TBD	
Escalate to Tier II?	TBD	TBD	
Provide Tier II technical support	TBD	TBD	
Escalate to Tier III?	TBD	TBD	
Provide Tier III technical support	TBD	TBD	
Resolution of trouble ticket	TBD	TBD	
Investigate & Diagnosis			
Verify user satisfaction with resolution	G5	G5	
Close trouble ticket	G5	G5	
Develop event, incident and problem filters	TBD	TBD	
Approve filters	G1	G1	
Access Management			
Determine rights			TBD
Validate request	G1	G1	G1
Request new PKI or change of rights			G5
Is new PKI required?	TBD	TBD	
Issue new PKI	TBD	TBD	
Change rights	TBD	TBD	
Issue Common Access Card (CAC)			G5
Provide physical access to seat			G5
Verify rights	TBD	TBD	TBD
Should access be granted?	G1	G1	G1
Log access or access attempt	TBD	TBD	TBD
Provide service	TBD	TBD	TBD
Notify originator	G5	G5	G5

G1 **The activity is a management control function and cannot be outsourced.**

TBD **To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**

G5 **The activity can be completely outsourced.**

No NetOps responsibilities.

11 NGEN Service Improvement

This section uses information from the *Continual Service Improvement* publication, the FRDC summarized in Annex C, and the service level management process for NGEN outlined in Annex H to determine NetOps responsibilities and level of DON authority over service improvement functions.

11.1 ITIL Service Improvement

The ITIL management process that supports service improvement in:

- **Service Level Management**. Includes service measurement and reporting as well as processes for reviewing existing service level agreements (SLAs) to determine whether changes are needed to support new or emerging operational requirements. [Annex H contains a more detailed discussion of service level management]

11.2 NGEN Service Improvement

Table 17 summarizes the governance, acquisition, and NetOps responsibilities for service improvement.

Table 17: Governance, Acquisition, and NetOps Responsibilities for Service Improvement

ITIL Management Function	Governance (DON CIO, OPNAV N6, and USMC C4)	Acquisition (PEO EIS)	NetOps (NETWARCOM and MCNOSC)
Service Level Management		✓ Develop SLAs; Develop OLA; and approve SLAs and OLAs	✓ Monitor service performance; review service requirements; and request new SLAs and OLAs

11.3 NetOps Service Improvement Authority

Table 18 combines the FRDC summarized in Annex C with the process outlined in Annex H to determine the level of DON authority over different NetOps management functions related to service improvement.

Table 18: Level of DON NetOps Authority over Service Improvement Functions

Service Improvement Management Functions	Global (GNOSC)	Regional (RNOSC/ITSC)	Local
Service Level Management			
Develop service requirements	TBD	TBD	
Approve service requirements	G1	G1	
Monitor and assess performance	G1	G1	
Review service requirements	TBD	TBD	
Modify service or operational level agreement?	G1	G1	
Develop service level agreements (SLAs)			
Develop operational level agreements (OLAs)			
Approve SLAs and OLAs			
Breach of SLAs and OLAs			
Develop service level management framework			
Approve framework			
Assign service level management responsibilities			
Analyze SLA/OLA breaches			
Assess framework			
Change framework?			

G1	**The activity is a management control function and cannot be outsourced.**
TBD	**To Be Determined. The activity could be a critical function, require a DON capability or require a DON competency.**
G5	**The activity can be completely outsourced.**
	No NetOps responsibilities.

12 NetOps Transition Challenges

This section outlines challenges associated with transitioning NetOps functions from NMCI to the NetOps construct for NGEN outlined in this CONOPS. Due to the significant differences between today's NMCI NetOps capabilities and what is required as well as the constraints of the acquisition process, the transition to the NetOps construct of this CONOPS will take place in phases, which will coincide with the NGEN block releases, to be completed by FOC.

12.1 NetOps Workforce Transition

12.1.1 In/Outsource Criteria

Four criteria were developed by the NGEN NetOps IPT and approved to determine whether the DON should perform a function or task:

- **Management Control**. The ability to direct, approve, monitor, and assess/evaluate – in support of decision making – IT services/functions are management control functions (i.e., inherently DON functions) that shall be retained by the DON. Additionally, the DON needs technical/subject matter expertise to support the assessment and evaluation, to an adequate level of depth which increases with the criticality of the decision or service, of the overall performance of contracted services. There is a subtle difference between the DON exerting management control over NGEN and the actual execution. For example, a contractor can develop a capacity plan. DON exerts management control by approving (or rejecting) the plan. A contractor, who could be the same one or a different one, can be responsible for executing the plan.
- **Critical function**. Those services or functions essential to the planning, mobilization, deployment, operational sustainment, and the transition phases of military operations (to include post-conflict operations). Loss or degradation of these functions jeopardizes the ability of the DON to execute the National Military Strategy.
- **DON capability**. Non-critical functions consist of those systems, services, and processes not directly related to military operations, and could be outsourced to a contractor. While not directly related to a mission essential task, these functions and services are important for basic network operations, and are typically specific to the vendor's implementation. The DON needs a basic capability to ensure continuity and success of critical operations in adverse conditions if the contractor providing these functions/services is unable to do so.
- **DON competency**. The DON needs to develop and maintain critical IT skills and competencies within certain service or functional areas.

Annex C contains a more detailed discussion of these FRDC.

12.1.2 Application of Criteria to NetOps Workforce

This CONOPS has identified those NetOps functions which are management control functions that shall be retained by the DON. Annexes D through U outline each ITILv3 management process for NGEN and identify the management control functions that shall be retained by the DON.[7] This analysis is reflected in Tables 10, 12, 14, 16, and 18 – which also identifies some functions the NetOps IPT had no reservations completely outsourcing.

The USMC considers SIPRnet a critical function essential to the planning, mobilization, deployment, operational sustainment, and transition phases of military operations. Consequently, as authorized by the Secretary of the Navy, the USMC SIPRnet will be a government owned and operated MD. The USN currently plans to outsource SIPRnet services as part of NGEN. Some of these services will be considered critical functions and require greater DON involvement than their unclassified counterparts.

The functions labeled as "TBD" (i.e., To Be Determined) in Tables 10, 12, 14, 16, and 18 need to be examined at a later date to determine if it is a critical function or a DON capability/competency is required and, if so, how many billets are associated with this requirement. Decisions about a DON capability or DON competency are dependent on the vendor solution cannot be made at this point in the acquisition cycle and will need to be re-visited at a later date. The DON also needs to determine whether, based on the analysis in Table 6.0 of the NGEN Requirements Document, SIPRnet is a critical function that cannot be outsourced.

The NGEN NetOps workforce will have to be developed in phases.

- **NGEN NetOps Workforce at IOC**.
  - DON personnel must be able to exert management control over NGEN.
- **NGEN NetOps Workforce at FOC**.
  - DON personnel will have assumed all critical functions, all functions that require a DON capability to mitigate operational risk, and all functions necessary to support the competencies needed for a sustainable DON IT workforce.

12.2 NGEN NetOps Capabilities Transition

NETWARCOM and MCNOSC have identified a requirement to support global, regional, and local NetOps capabilities to meet their operational requirements. These capabilities must be approved and developed by the Technical Design Authority (TDA) in phases:

- **NGEN NetOps Capabilities at IOC**.
  - Support the separate USN and USMC MDs outlined in this CONOPS.
  - Support all global NetOps capabilities and ITSM functions outlined in this CONOPS.
  - Implement management controls based on the FRDC criteria (summarized in Annex C) and those NetOps/ITSM functions needed to support these management controls.

[7] Each annex also provides use cases that illustrate how each management process will function.

- **NGEN NetOps Capabilities at FOC**.
  - Support all of the regional and local NetOps capabilities and ITSM functions outlined in this CONOPS.
  - Integration of NGEN NetOps capabilities into existing NCTAMS/NCTS structure.

A Abbreviations and Acronyms

C2	Command and Control
CAC	Common Access Card
CARS	Cyber Asset Reduction and Security
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRT	Computer Incident Response Team
CM	Content Management
CMC	Commandant of the Marine Corps
CND	Computer Network Defense
CND RA	Computer Network Defense Response Actions
COMMARFOR	Commander of Marine Forces
COOP	Continuity of Operations
COI	Community of Interest
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DON	Department of the Navy
EAG	Enterprise Advisory Group
EIS	Enterprise Information Systems
EITC	Enterprise Information Technology Support Center
EM	Enterprise Management
E-mail	Electronic Mail
ESG	Executive Steering Group
FNA	Functional Needs Assessment
FOC	Full Operational Capability
FRDC	Function Responsibility Decision Criteria
GIG	Global Information Grid
GNO	Global Network Operations
GNOSC	Global Network Operations and Security Center
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance

IM	Information Management
IOC	Initial Operating Capability
IPT	Integrated Product Team
IT	Information Technology
IT-21	Information Technology for the 21st Century
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JTF	Joint Task Force
LNC	Legacy Network Consolidation
MAGTF	Marine Air-Ground Task Force
MARCORSYSCOM	Marine Corps Systems Command
MCEITS	Marine Corps Enterprise IT Services
MCEN	Marine Corps Enterprise Network
MCI	Marine Corps Installation
MCNOSC	Marine Corps Network Operations and Security Center
MD	Management Domain
MHQ with MOC	Maritime Headquarters with Maritime Operations Center
MITSC	MAGTF Information Technology Support Center
MOC	MCEITS Operation Center
NCES	Net-Centric Enterprise Services
NCTAMS	Navy Computer and Telecommunications Area Master Station
NCTS	Navy Computer and Telecommunications Station
ND	Network Defense
NETWARCOM	Naval Network Warfare Command
NGEN	Next Generation Enterprise Network
NIPRnet	Non-Classified Internet Protocol Router Network
NITSC	Navy Information Technology Support Center
NMCI	Navy Marine Corps Intranet
NNE	Naval Networking Environment
NOC	Network Operations Center
OAG	Operational Advisory Group
OLA	Operating Level Agreement
ONE-NET	OCONUS Navy Enterprise Network
OPCON	Operational Control

PEO	Program Executive Office
PKI	Public Key Infrastructure
RNOSC	Regional Network Operations and Security Center
SIPRnet	Secure Internet Protocol Router Network
SLA	Service Level Agreement
TACON	Tactical Control
TAG	Technical Advisory Group
TDA	Technical Design Authority
TNOSC	Theater Network Operations and Security Center
TYCOM	Type Commander
USMC	United States Marine Corps
USN	United States Navy
USSTRATCOM	United States Strategic Command
WFNS	Warfighter Network Services

B Glossary

Application	Software that runs on a server or client and provides functions needed by an IT service.
Community of Interest (COI)	A group of users that collaborate in support of a common operational (e.g. Surface Warfare, Amphibious Operations, Joint Task Force, etc.) or functional (e.g., logistics, personnel, medical, training, etc.) objective. A COI can include users from a single MD, multiple MDs, network, or multiple networks.
Concept of Operations (CONOPS)	A description of how a set of capabilities may be employed to achieve desired objectives or a particular end state. A CONOPS synthesizes the details of who, where, and most importantly, how a mission or objectives are to be accomplished from naval operational concepts, doctrine, and capabilities.
Event	A change of state that is of significant importance to the management of an IT service.
Incident	An unplanned interruption to or reduction in quality of an IT service.
IT Service	A combination of people, processes, and technology that support operations. IT services have performance objectives established by a set of service level agreements.
Management Control	The ability to direct, approve, monitor, and assess/evaluate – in support of decision making – IT services/functions are management control functions (i.e., inherently DON functions) that shall be retained by the DON. Additionally, the DON needs technical/subject matter expertise to support the assessment and evaluation, to an adequate level of depth which increases with the criticality of the decision or service, of the overall performance of contracted services. There is a subtle difference between the DON exerting management control over NGEN and the actual execution. For example, a contractor can develop a capacity plan. DON exerts management control by approving (or rejecting) the plan. A contractor, who could be the same one or a different one, can be responsible for executing the plan.
Management Domain (MD)	Boundaries within a network for which a management authority will effect NetOps command and control. MDs are designated by the network's Service component command authority or Service Headquarters and include within them the ability to direct and manage network resources and capabilities.
Naval Networking Environment (NNE)	Multiple DON networks that benefit from interoperability – the standardization of capabilities and services – to support achievement of net-centric objectives.

Network	Multiple connected computers that communicate over a wired or wireless medium to share data, as well as other resources, and are under the control of a Service component command authority. A network represents the totality of voice, video, and data services infrastructure from wide area network to desktops.
Network Operations (NetOps)	Encompasses all activities associated with operating and defending networks, their applications, and their services.
Operational Control (OPCON)	Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. OPCON is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. OPCON includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. OPCON should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. OPCON provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training.
Problem	The cause of one or more incidents.
Tactical Control (TACON)	Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. TACON is inherent in OPCON. TACON may be delegated to, and exercised at any level at or below the level of combatant command. TACON provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task.

C Functional Responsibility Decision Criteria

NGEN will be managed by the DON with contractor support. Many of the NetOps problems with NMCI resulted from the inability of the DON to exert operational control over NMCI. Too many management functions were outsourced to the contractor in NMCI. To correct these problems, the DON must have a much larger role in the operation and management of NGEN, and must "own" critical NGEN services or functions.

The following decision criteria will be used to determine whether an NGEN service or function should be owned and/or operated by the DON: management control (DON must do), critical function (DON must do), DON capability (DON capability needed to mitigate operational risk), and DON competency (DON capability needed to support growth and development of its IT workforce).

C.1 Management Control

The ability to direct, approve, monitor, and assess/evaluate – in support of decision making – IT services/functions necessary to exert management control over NGEN and are inherently DON functions. The DON must retain these management controls to ensure that NGEN is responsive to the evolving operational requirements and mission objectives of the commands it supports. Additionally, the DON needs technical/subject matter expertise to support the assessment and evaluation – to an adequate level of depth which increases with the criticality of the decision or service – of the overall performance of contracted services. The following criteria are used to determine whether a NGEN service or function involves management control of NGEN and, therefore, must be retained by the DON:

- **Does it involve directing DON personnel?** DON personnel are prohibited by law from being directed by a contractor.
- **Does it involve approval authority or overall direction of activities?** The DON shall retain approval authority and overall direction of NGEN policies, plans, architectures, standards, requirements, contracts, operations, resources, and funding.
- **Does it involve monitoring or assessing overall performance of contracted services?** The DON shall retain the ability to monitor and assess contracted services to verify service level agreements (SLAs) and operating level agreements (OLAs) are being met.
- **Does it involve decisions regarding acceptance of significant risk?** The DON must make decisions about how much risk it is willing to accept in operations, security, the development of new capabilities, and force management.

C.2 Critical Function

Those services or functions essential to the planning, mobilization, deployment, operational sustainment, and the transition phases of military operations (to include post-conflict operations). Loss or degradation of these functions jeopardizes the ability of the DON to execute the National Military Strategy. The following criteria are used to determine whether an NGEN service or function is critical:

- **Is it a critical enabler of defined DON core competencies?** U.S. Marine Corps core competencies are warfighting culture and dynamic decision making; expeditionary forward operations; sustainable and interoperable littoral power projection; combined arms integration; and forcible entry from the sea. U.S. Navy core competencies are forward naval presence; deterrence; sea control; power projection; maritime security; and humanitarian assistance/disaster response. The mission essential tasks associated with these core competencies depend on various network, services, and functions. The DON shall retain network and service functions that are critical enablers of core competencies.
- **Is it unique to the military mission or difficult for industry to fully accomplish?** For example, network services and functions that deploy with military forces are unique to the military mission and would be difficult for contractors to fully support. Consequently, these network services and functions shall be retained by the DON.

C.3 DON Capability

Non-critical functions consist of those systems, services, and processes not directly related to military operations, and could be outsourced to a contractor. While not directly related to a mission essential task, these functions and services are important for basic network operations, and are typically specific to the contractor's implementation. The DON needs a basic capability to ensure continuity and success of critical operations in adverse conditions if the contractor providing these functions/services is unable to do so. The following criteria are used to determine whether a DON capability is needed to support a service or function:

- **Is it a unique and critical non-military core competency that requires DON expertise or resources to mitigate operational risk?** There may be situations (e.g., natural disaster, risk of war/civil unrest, etc.) when contractors are evacuated, but there is still a need to provide the NGEN service or function. Consequently, the DON shall maintain a basic capability to support the continuity of critical operations.
- **Does it require continuous augmentation or training/planning for emergency augmentation by the DON?** Continuous augmentation is required when the skills or knowledge associated with the capability are extremely perishable. In this case, the DON needs to provide continuous augmentation of the contractor to ensure it has the required capability. However, if the skills or knowledge are not perishable, the DON can train and plan for emergency augmentation without requiring DON personnel to be embedded with the contractor.

C.4 DON Competency

The DON needs to develop and maintain critical IT skills and competencies within certain service or functional areas. The following criteria are used to determine whether a DON competency is required:

- **Are these skills needed for career progression into billets associated with critical and management control functions?** The DON shall retain a sufficient number of billets within NGEN to grow the expertise needed to support management control and critical functions.

- **Does performance of the function support retention or enhancement of critical IT skills used in the deployed environment?** The DON shall retain a sufficient number of billets within NGEN to ensure individuals rotating from a deployed environment are able to maintain their core IT skills and competencies while at a shore-based assignment.

D Financial Management

Figure 9: NGEN Processes for Financial Management

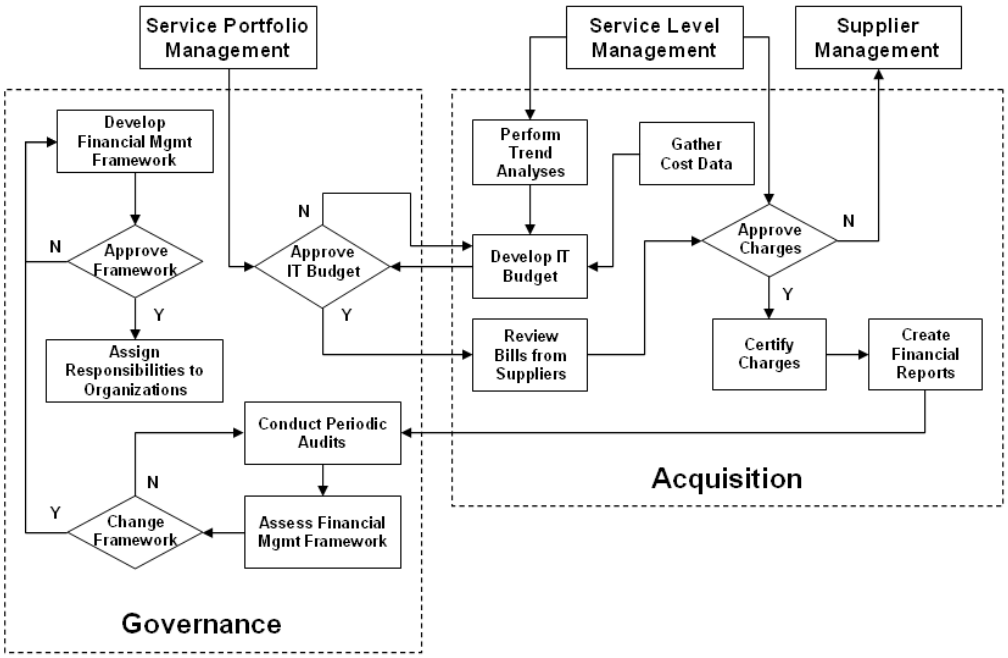


Figure 9 provides a high-level overview of the NGEN processes associated with financial management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 9, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

D.1 NGEN NetOps Authority

There are no NetOps decision points or tasks within the financial management processes outlined in Figure 9.

E Demand Management

Figure 10: NGEN Processes for Demand Management

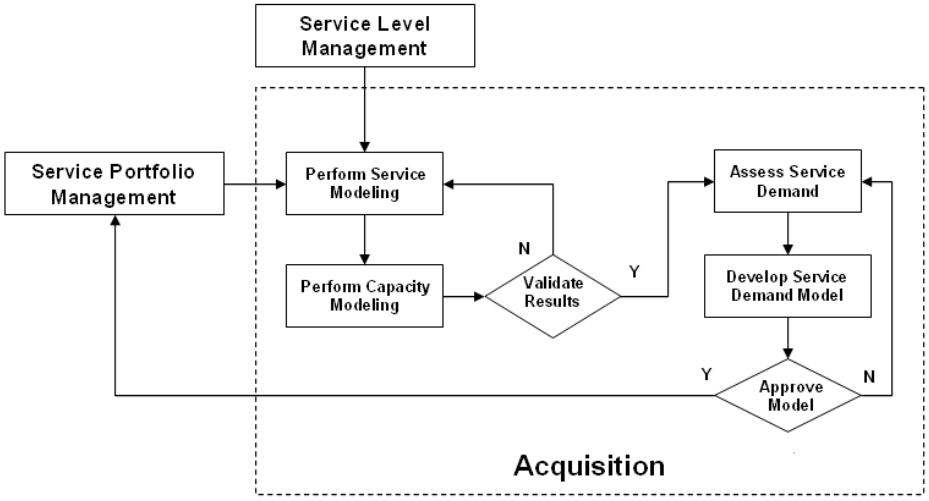


Figure 10 provides a high-level overview of the NGEN processes associated with demand management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 10, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

E.1 NGEN NetOps Authority

There are no NetOps decision points or tasks within the demand management processes outlined in Figure 10.

F Service Portfolio Management

Figure 11: NGEN Processes for Service Portfolio Management

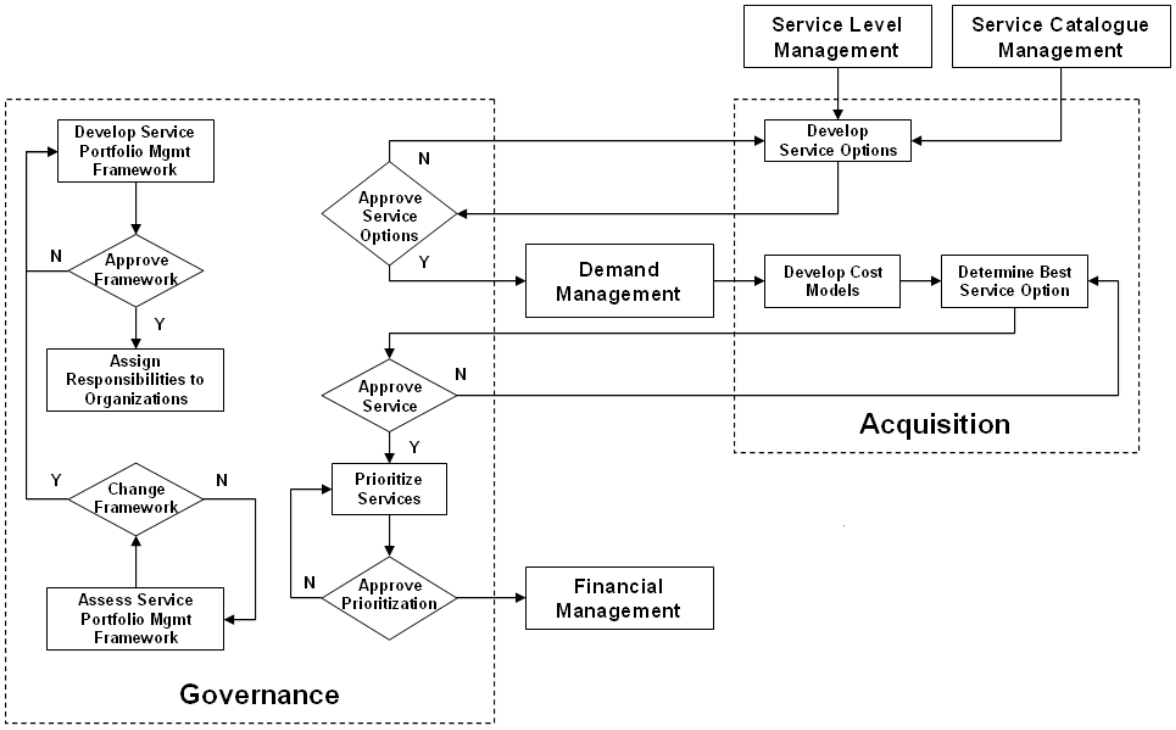


Figure 11 provides a high-level overview of the NGEN processes associated with service portfolio management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 11, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

F.1 NGEN NetOps Authority

There are no NetOps decision points or tasks within the service portfolio management processes outlined in Figure 11.

G Service Catalogue Management

Figure 12: NGEN Processes for Service Catalogue Management

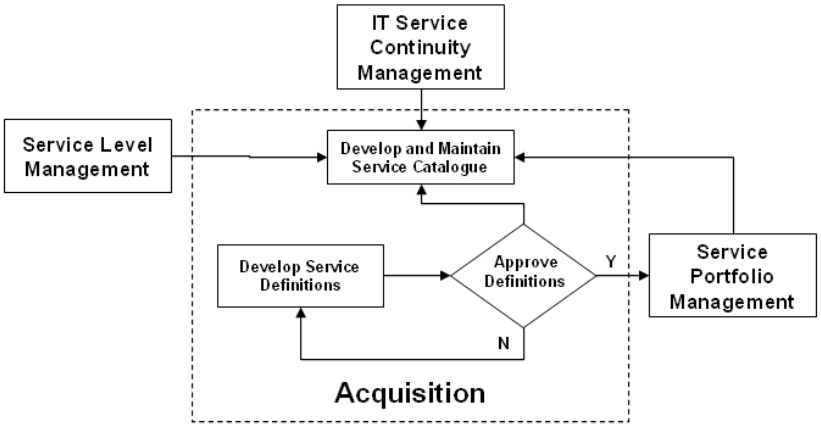


Figure 12 provides a high-level overview of the NGEN processes associated with service catalogue management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 12, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

G.1 NGEN NetOps Authority

There are no NetOps decision points or tasks within the service catalogue management processes outlined in Figure 12.

H Service Level Management

Figure 13: NGEN Processes for Service Level Management

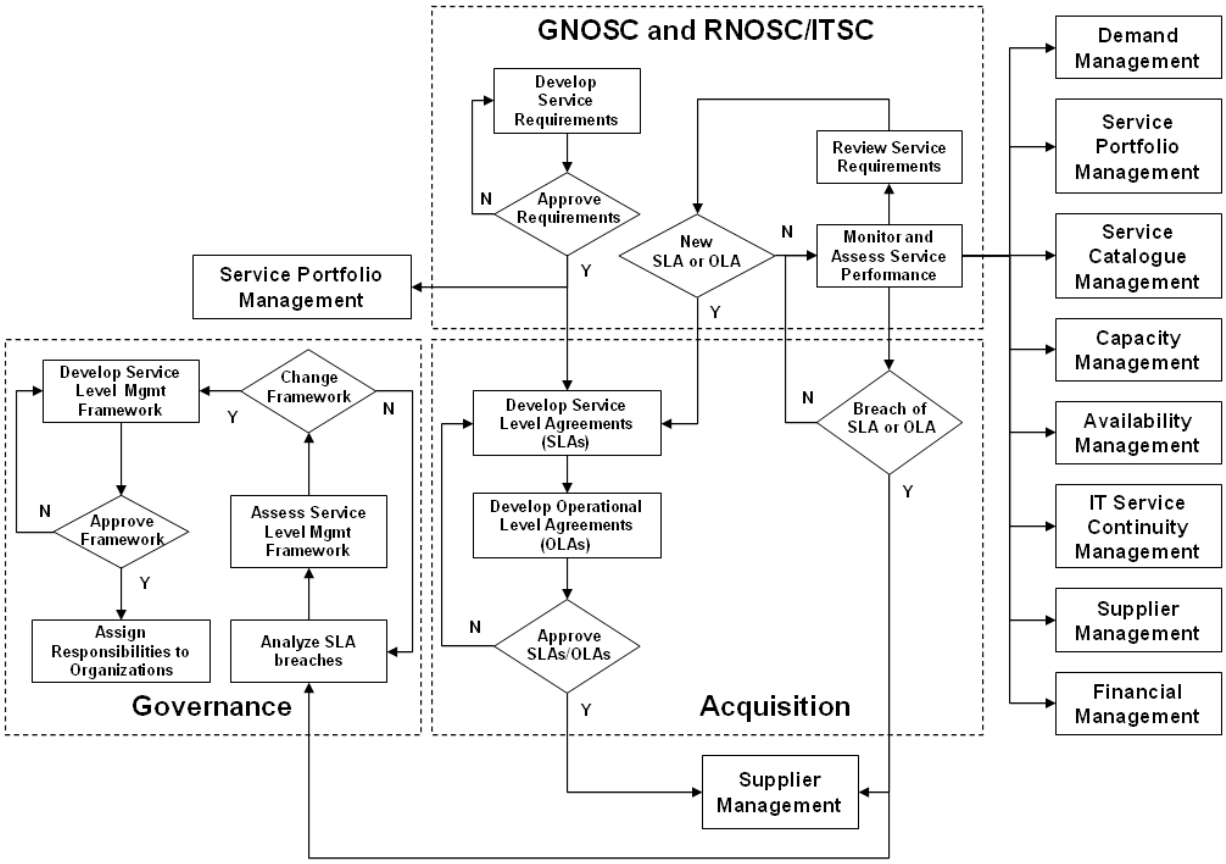


Figure 13 provides a high-level overview of the NGEN processes associated with service level management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 13, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

H.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the service level management processes outlined in Figure 13 must be retained by the DON:

- **Approve service requirements.** Approval authority over requirements is a management control function that shall be retained by the DON.

- **Monitor and assess service performance.** The ability to monitor and assess contracted services is a management control function that shall be retained by the DON.
- **New service level agreement (SLA) or operational level agreement (OLA).** Approval authority and direction over NGEN requirements and contracts is a management control function that shall be retained by the DON.

H.2 Use Case: New Enterprise-Class Collaboration Service

Based on Figure 13, the process for developing a new enterprise-class service is:

- **Develop service requirement.** The GNOSC or RNOSC/ITSC develop a requirement for an enterprise-class collaboration service.
- **Approve service requirement.** The GNOSC, or responsible Service organization, approves the requirements for the collaboration service and passes them to the acquisition authority.
- **Develop SLAs.** The acquisition authority develops SLAs based on the service requirements provided by the GNOSC.
- **Develop OLAs.** The acquisition authority develops OLAs based on the service requirements provided by the GNOSC.
- **Approve SLAs and OLAs.** The acquisition authority approves of the SLAs and OLAs for the service and passes them to the supplier management process for source selection.

H.3 Use Case: New requirement for Enterprise-Class Collaboration Service

Based on Figure 13, the process for developing new requirements for an existing enterprise-class collaborative service is:

- **Monitor and assess service performance.** Through its monitoring and assessment functions, the GNOSC notices usage of the service has increased dramatically due to creation of a Joint Task Force (JTF) in support of an ongoing operation.
- **Review service requirements.** The GNOSC determines the current requirement for the number of concurrent users supported is too low and increases the requirement.
- **New SLAs and OLAs are required.** The GNOSC determines that new SLAs and OLAs are required to meet the new requirement.
- **Develop SLAs.** The acquisition authority develops modifications to the existing SLAs based on the new requirement.
- **Develop OLAs.** The acquisition authority develops modifications to the existing OLAs based on the new requirement.
- **Approve SLAs and OLAs.** The acquisition authority approves of the modifications to the SLAs and OLAs for the service and passes them to the supplier management process for re-negotiation with the vendor.

H.4 Use Case: Breach of SLA for Enterprise-Class Collaboration Service

Based on Figure 13, the process for determining a SLA/OLA breach for an existing enterprise-class collaborative service is:

- **Monitor and assess service performance.** Through its monitoring and assessment functions, the GNOSC notices usage of the service is low and it has received complaints via the Service Desk from users that have problems accessing the enterprise-class collaboration service.
- **Breach of SLA.** The acquisition authority examines the contract language of the SLA and the data/assessment from the GNOSC. The acquisition authority determines the vendor has not met the SLA for the number of concurrent users supported and passes the breach to the supplier management for resolution.
- **Analyze SLA breaches.** The governance authority examines all SLA and OLA breaches for trends.
- **Assess service level management framework.** The governance authority conducts an assessment to determine if the number or types of SLA/OLA breaches suggest the current framework for service level management needs to be changed.
- **No change to framework is needed.** The governance authority determines the current service level management framework is functioning adequately and no changes to it are necessary at this time.

I Capacity Management

Figure 14: NGEN Processes for Capacity Management

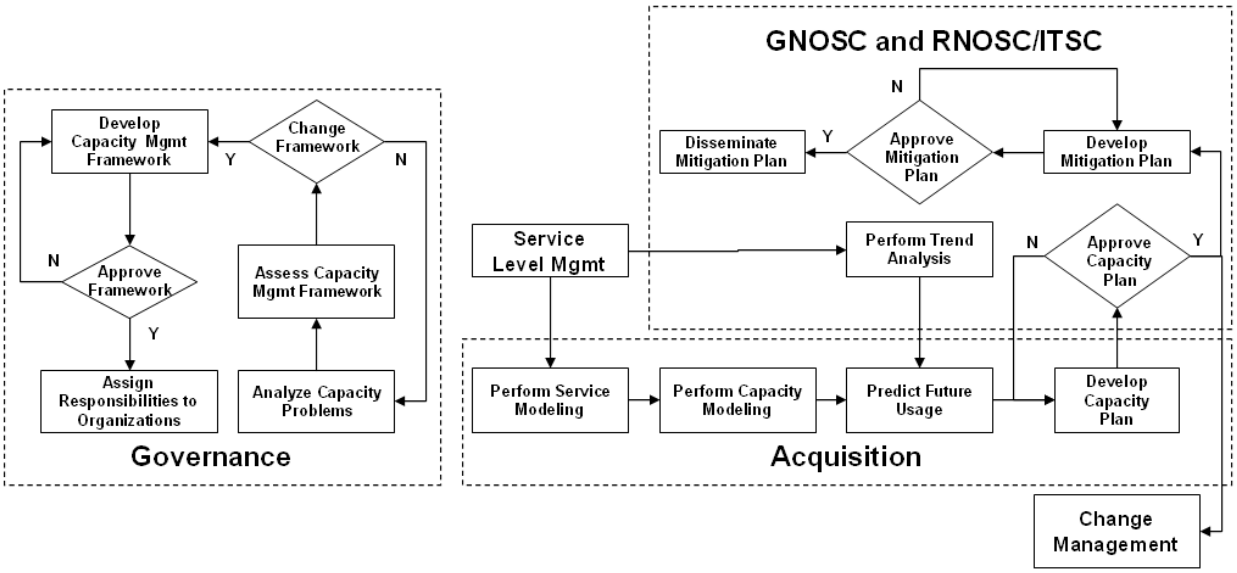


Figure 14 provides a high-level overview of the NGEN processes associated with capacity management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 14, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

I.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the capacity management processes outlined in Figure 14 must be retained by the DON:

- **Approve capacity plan.** Approval authority over NGEN plans is a management control function that shall be retained by the DON.
- **Approve mitigation plan.** Approval authority over NGEN plans is a management control function that shall be retained by the DON.

I.2 Use Case: Projected Capacity Shortfall

Based on Figure 14, the process for acquiring more capacity is:

- **Perform trend analysis.** The NetOps authority performs basic trend analysis using capacity/service usage data. The analysis shows a capacity shortfall in six months.

- **Predict future capacity.** The acquisition authority combines the basic trend analysis of from the NetOps authority with its own modeling to predict future capacity usage and adjusts the shortfall date by an additional two months with its more detailed analysis.
- **Develop capacity plan.** The acquisition authority develops a plan to procure capacity.
- **Approve capacity plan.** The NetOps authority approves the capacity plan and submits a Request for Change (RFC) to the change management process.
- **Develop mitigation plan.** The NetOps authority develops a plan for how it will address the capacity shortfall by reducing service and/or user demand for capacity.
- **Approve mitigation plan.** The NetOps authority approves the measures proposed in the mitigation plan for addressing the capacity shortfall.

J Availability Management

Figure 15: NGEN Processes for Availability Management

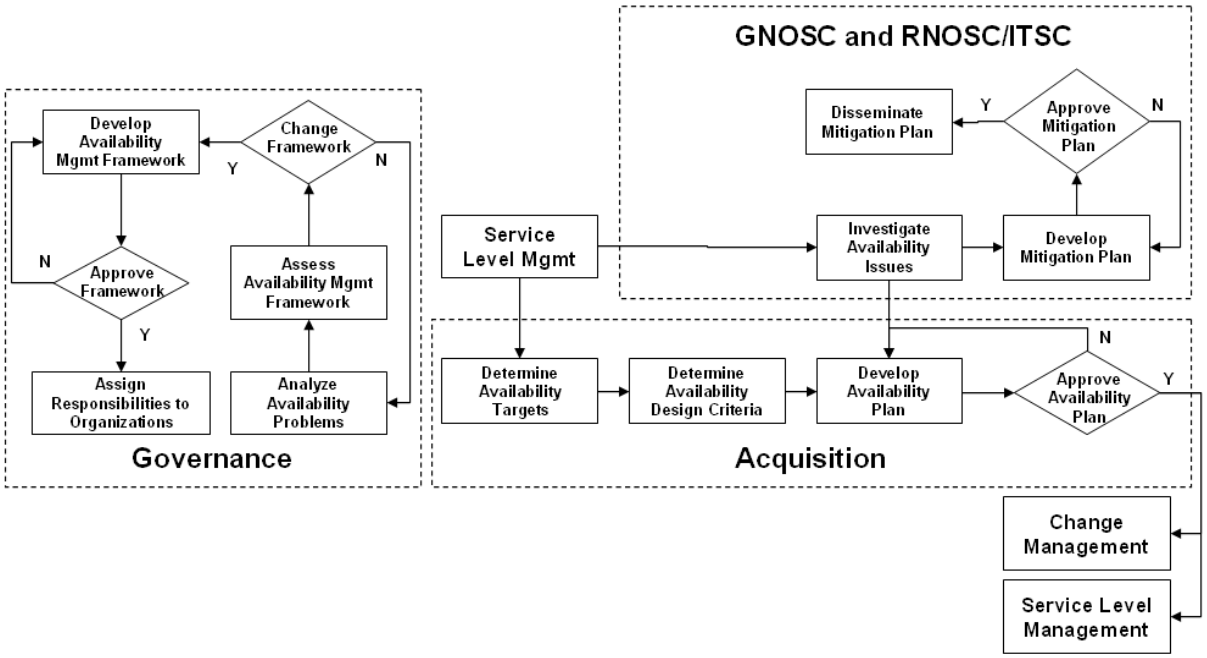


Figure 15 provides a high-level overview of the NGEN processes associated with availability management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 15, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

J.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the availability management processes outlined in Figure 15 must be retained by the DON:

- **Approve mitigation plan.** Approval authority over NGEN plans is a management control function that shall be retained by the DON.

K IT Service Continuity Management

Figure 16: NGEN Processes for IT Service Continuity Management

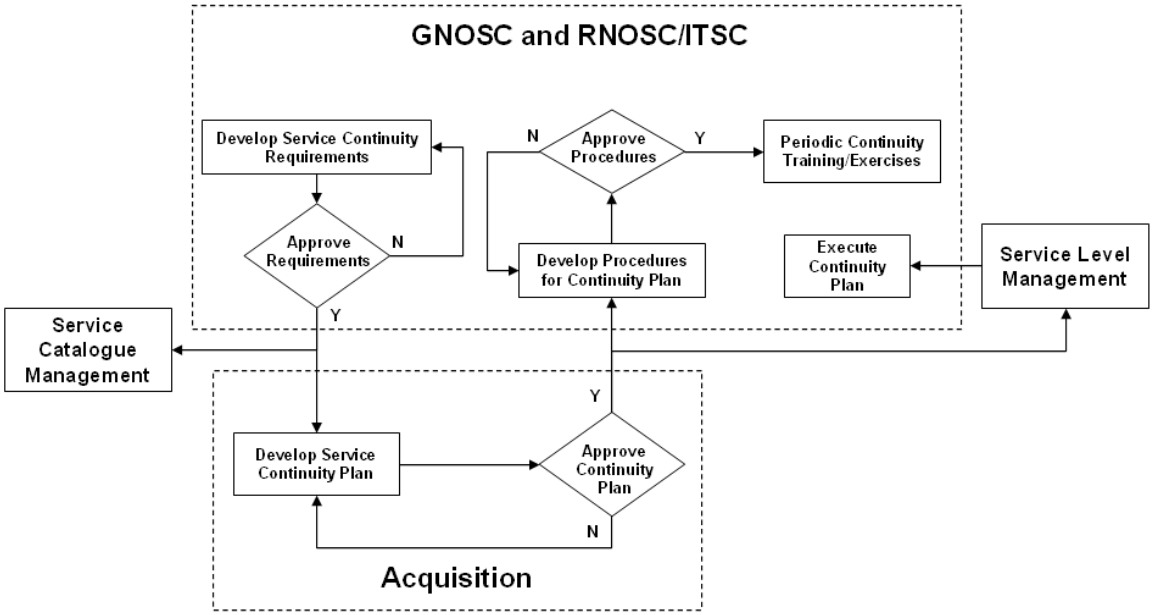


Figure 16 provides a high-level overview of the NGEN processes associated with IT service continuity management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 16, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

K.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the IT service continuity management processes outlined in Figure 16 must be retained by the DON:

- **Approve requirements.** Approval authority over NGEN requirements is a management control function that shall be retained by the DON.
- **Approve procedures.** Approval authority over NGEN operations is a management control function that shall be retained by the DON.
- **Execute continuity plan.** Overall direction of NGEN operations is a management control function that shall be retained by the DON. The execution of continuity plans may be automated as long as the appropriate NetOps authority can specify the criteria which determine when the continuity plan is executed.

L Information Security Management

Figure 17: NGEN Processes for Information Security Management

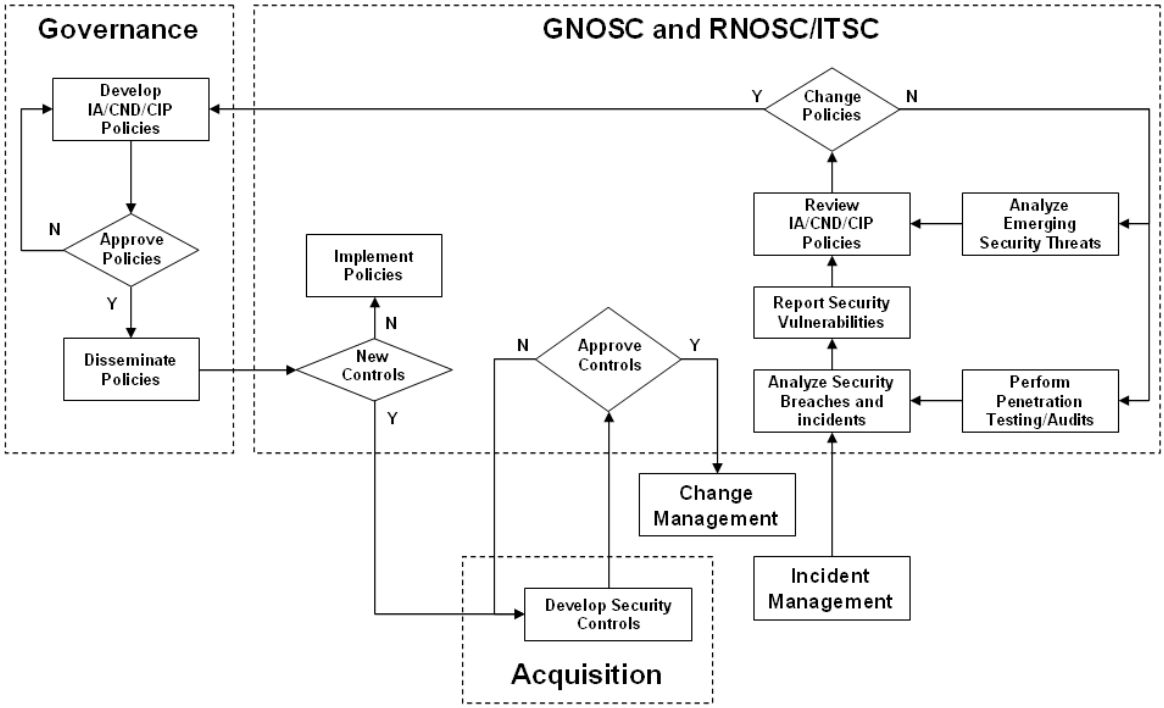


Figure 17 provides a high-level overview of the NGEN processes associated with information security management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 17, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

L.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the information security management processes outlined in Figure 17 must be retained by the DON:

- **New controls.** Approval authority over NGEN requirements is a management control function that shall be retained by the DON.
- **Approve controls.** Approval authority over NGEN operations is a management control function that shall be retained by the DON.
- **Change policies.** Approval authority over NGEN policies is a management control function that shall be retained by the DON.

M Supplier Management

Figure 18: NGEN Processes for Supplier Management

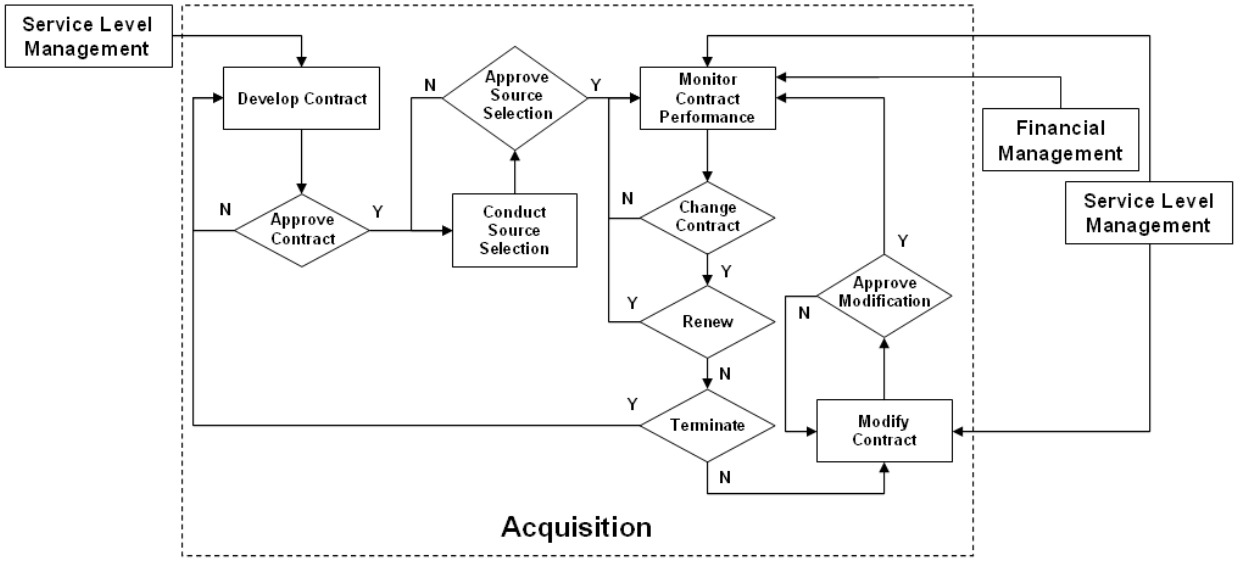


Figure 18 provides a high-level overview of the NGEN processes associated with supplier management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 18, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

M.1 NGEN NetOps Authority

There are no NetOps decision points or tasks within the supplier management processes outlined in Figure 18.

N Change Management

Figure 19: NGEN Processes for Change Management

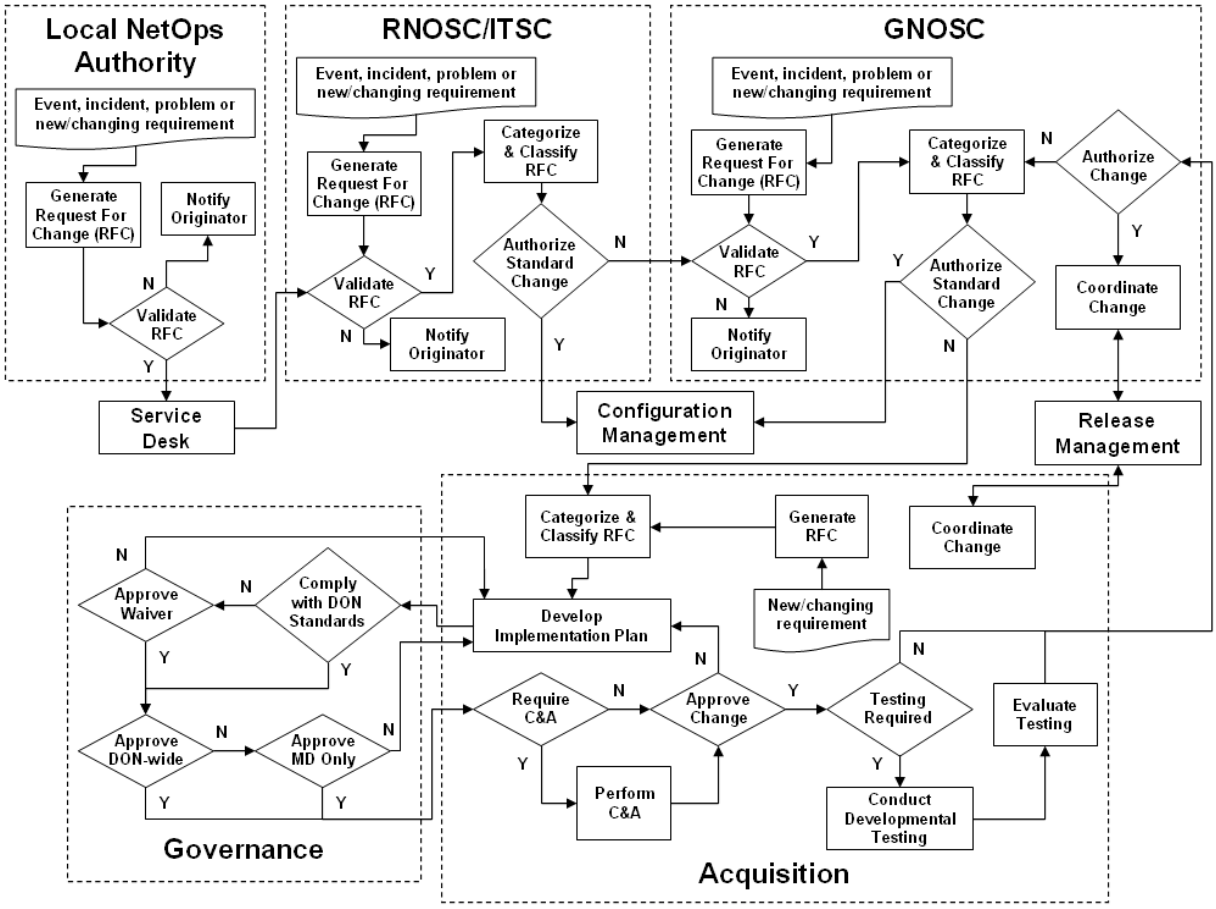


Figure 19 provides a high-level overview of the NGEN processes associated with change management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 19, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

N.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the change management processes outlined in Figure 19 must be retained by the DON:

- **Validate RFC.** Approval authority over NGEN requirements is a management control function that shall be retained by the DON.

- **Authorize standard change.** Approval authority over NGEN operations is a management control function that shall be retained by the DON.
- **Authorize change.** Approval authority over NGEN architectures is a management control function that shall be retained by the DON.

N.2 Use Case: Request Additional Storage Resources

Based on Figure 19, the process for increasing storage resources:

- **New requirement.** A command needs additional file storage space to support a Joint Task Force (JTF).
- **Generate a RFC.** The command generates a RFC based on the new requirements.
- **Validate the RFC.** The command validates the RFC and sends it to the service desk.
- **Validate the RFC.** The RNOSC/ITSC receives the RFC from the service desk and validates it.
- **Categorize & Classify RFC.** The RNOSC/ITSC categorizes the RFC as a high-priority change because it is an operational necessity for supporting a JTF.
- **RFC is a minor change.** The RFC involves increasing the amount of file storage available to the command and, since the RNOSC/ITSC is responsible for apportioning these resources, the RFC is a minor change (i.e., configuration change).
- **Forward to configuration management.** The RFC is sent to configuration management to increase the file space the command has access to.

N.3 Use Case: Request for New Collaboration Tool

Based on Figure 19, the process for obtaining a new collaborative tool:

- **New requirement.** A command needs a new collaborative tool to support a JTF.
- **Generate a RFC.** The command generates a RFC based on the new requirements.
- **Validate the RFC.** The command validates the RFC and sends it to the service desk.
- **Validate the RFC.** The RNOSC/ITSC receives the RFC from the service desk and validates it.
- **Categorize & Classify RFC.** The RNOSC/ITSC categorizes the RFC as a high-priority change because it is an operational necessity for supporting a JTF.
- **RFC is not a minor change.** The RFC involves the installation of a new application and is therefore not considered a minor change (i.e., configuration change) and forwarded to the GNOSC for review.
- **Validate the RFC.** The GNOSC validates the RFC.
- **Categorize & Classify RFC.** The GNOSC concurs with the RNOSC/ITSC categorization of the RFC as a high-priority change.

- **RFC is not a standard change.** The RFC involves the installation of a new application and is therefore not considered a standard change. The RFC is forwarded to the acquisition community for review.
- **Categorize & Classify RFC.** The acquisition authority concurs with the GNOSC and RNOSC/ITSC categorization of the RFC as a high-priority change.
- **Develop an implementation plan.** The acquisition authority develops a plan to install the new application on six seats at the command.
- **Does not comply with DON standards.** The governance authority determines the new application does not comply with DON standards.
- **Grant a waiver.** The governance authority grants a one-year waiver due to the urgent operational need that resulted in the RFC.
- **Certification & accreditation.** The acquisition authority completes C&A documentation and forwards it to the DAAs who authorize the application to run on USN and USMC NGEN MDs.
- **Approve change.** The acquisition community approves the change.
- **Testing is not required.** Based on operational testing from the U.S. Air Force and Army, as well as approval by the DAAs, the acquisition community determines additional DON testing is not required.
- **Approve change.** The GNOSC approves the change.
- **Coordinate change.** The GNOSC notifies the RNOSC/ITSC, command, and acquisition community of change approval.
- **Forward to release management.** The RFC and implementation plan are forwarded to the release management process.

O Release Management

Figure 20: NGEN Processes for Release Management

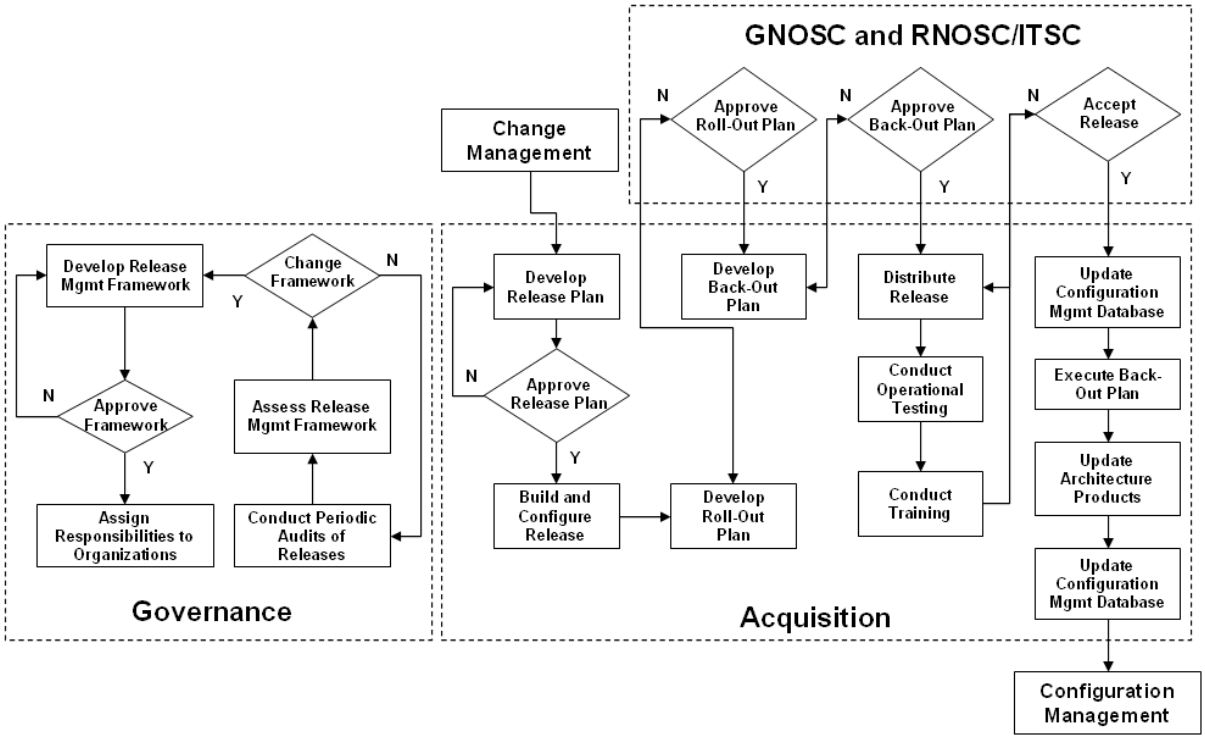


Figure 20 provides a high-level overview of the NGEN processes associated with release management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 20, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

O.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the release management processes outlined in Figure 20 must be retained by the DON:

- **Approve roll-out plan.** Approval authority over NGEN plans is a management control function that shall be retained by the DON.
- **Approve back-out plan.** Approval authority over NGEN plans is a management control function that shall be retained by the DON.

- **Accept release.** Approval authority over NGEN operations is a management control function that shall be retained by the DON.

O.2 Use Case: Release for New Collaboration Tool

Based on Figure 20, the process for releasing the collaborative tool outlined in an Annex N use case is:

- **Develop release plan.** The acquisition authority develops a release plan to install a new collaboration tool on six seats at a command.
- **Approve release plan.** The acquisition authority approves of the release plan.
- **Develop a roll-out plan.** The acquisition community develops a plan to roll-out the release at the command.
- **Approve roll-out plan.** The GNOSC approves the roll-out plan.
- **Develop a back-out plan.** The acquisition community develops a plan to remove the new application if/when necessary should the install fail.
- **Approve back-out plan.** The GNOSC approves the back-out plan.
- **Distribute release.** The acquisition community distributes the application to the command for installation.
- **Conduct testing.** The command verifies it can use the collaborative application to interact with the JTF.
- **Conduct training.** The acquisition community has arranged for U.S. Army personnel familiar with the application to train users at the command.
- **Accept release.** Based on positive feedback from the command, the GNOSC accepts the release of the new application.
- **Update configuration management database.** The configuration management database is updated to reflect the new release.
- **Execute back-out plan.** The acquisition community executes the back-out plan when appropriate (e.g., the JTF is disestablished, the waiver expires, etc.).
- **Update architecture products.** Architecture products are updated, when required, to reflect changes to the architecture and Configuration Management is notified.
- **Update configuration management database.** The configuration management database is updated to reflect changes or removal of the collaborative application from the six seats.

P Configuration Management

Figure 21: NGEN Processes for Configuration Management

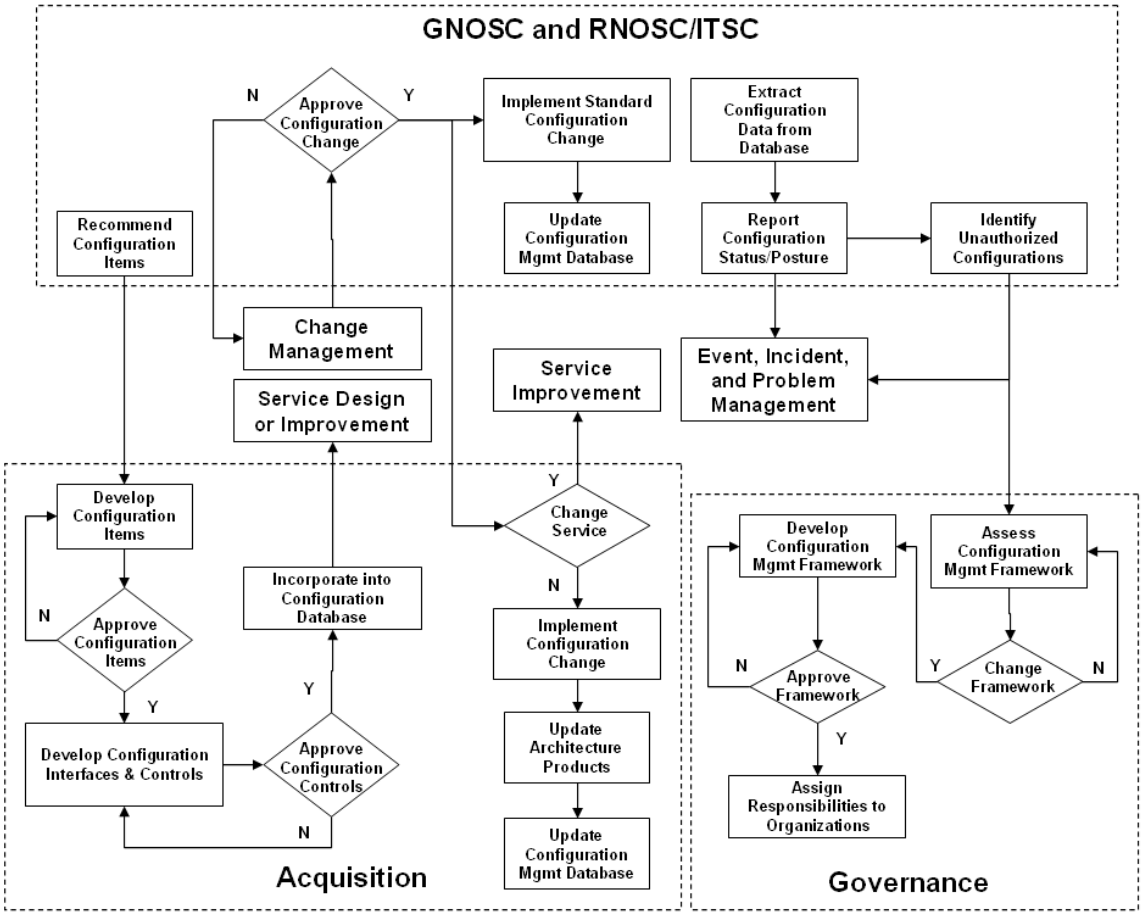


Figure 21 provides a high-level overview of the NGEN processes associated with configuration management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 21, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

P.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the configuration management processes outlined in Figure 21 must be retained by the DON:

- **Approve configuration change.** The ability to direct NGEN operations is a management control function that shall be retained by the DON.

P.2 Use Case: Request Additional Storage Resources

Based on Figure 21, the process for increasing storage resources, as outlined in one of the use cases in Annex N:

- **Approve configuration change.** A RNOSC/ITSC approves the configuration change to increase the file storage space of the command in support of a Joint Task Force (JTF).
- **Implement standard configuration change.** The RNOSC/ITSC is responsible for apportioning file storage resources and, since the configuration change only changes the current apportionment, it is considered a minor change. If there is sufficient excess storage space, the increase in the command apportionment will come from the storage reserve. However, if all the storage space has been apportioned, the RNOSC/ITSC will have to reduce the storage apportionment of other commands to satisfy the request.
- **Update the configuration database.** . The RNOSC/ITSC informs Configuration Management to update the configuration management database to reflect the new file storage apportionment.

P.3 Use Case: Upgrade Mail Server Software

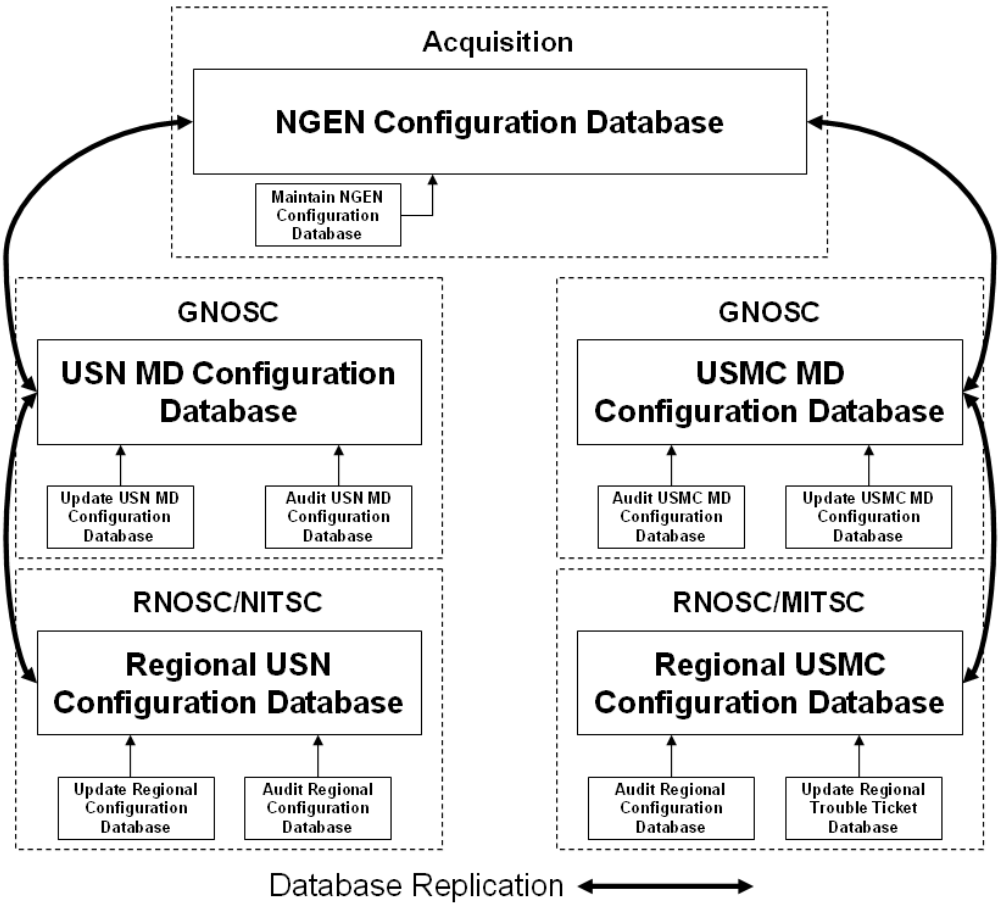
Based on Figure 21, the process for upgrading the mail server software, as outlined in one of the use cases in Annex N:

- **Tasking from JTF-GNO.** JTF-GNO has requested the server software on all Microsoft Exchange servers be upgraded due to a buffer overflow threat.
- **Approve configuration change.** The GNOSC approves the configuration change to the server software.
- **Not a standard configuration change.** Upgrading the server software is not a minor change and the acquisition authority needs to be involved.
- **The existing mail service does not need to be changed.** The server software needs to be upgraded, which does not require changes to the existing mail service (i.e., no additional servers, change to the architecture, etc.).
- **Implement configuration change.** Assuming the funding is available, the acquisition authority implements the configuration change through the change and release management processes.
- **Update architecture products.** Architecture products are updated, when required, to reflect changes to the architecture.
- **Update the configuration database.** The acquisition authority notifies Configuration Management to update the configuration management database to reflect the new mail server software.

P.4 Federated Configuration Database

Figure 22 depicts a federated NGEN configuration database system. With this federated architecture, the technical design authority maintains a master configuration database that contains configuration information from both the USN and USMC MDs. Each NGEN MD then maintains its own configuration database at the GNOSC, which synchronizes its configuration items with the master database. Regional RNOSC/ITSCs also maintain their own regional configuration database, which synchronizes its configuration items with the larger databases at the GNOSC. The replication of configuration items between these databases allows each NetOps authority to maintain and audit the portions of the master configuration database and the replication process ensures any changes are quickly reflected in the configuration database for the MD and the master NGEN configuration database.

Figure 22: Federated NGEN Configuration Databases



Q Event Management

Figure 23: NGEN Processes for Event Management

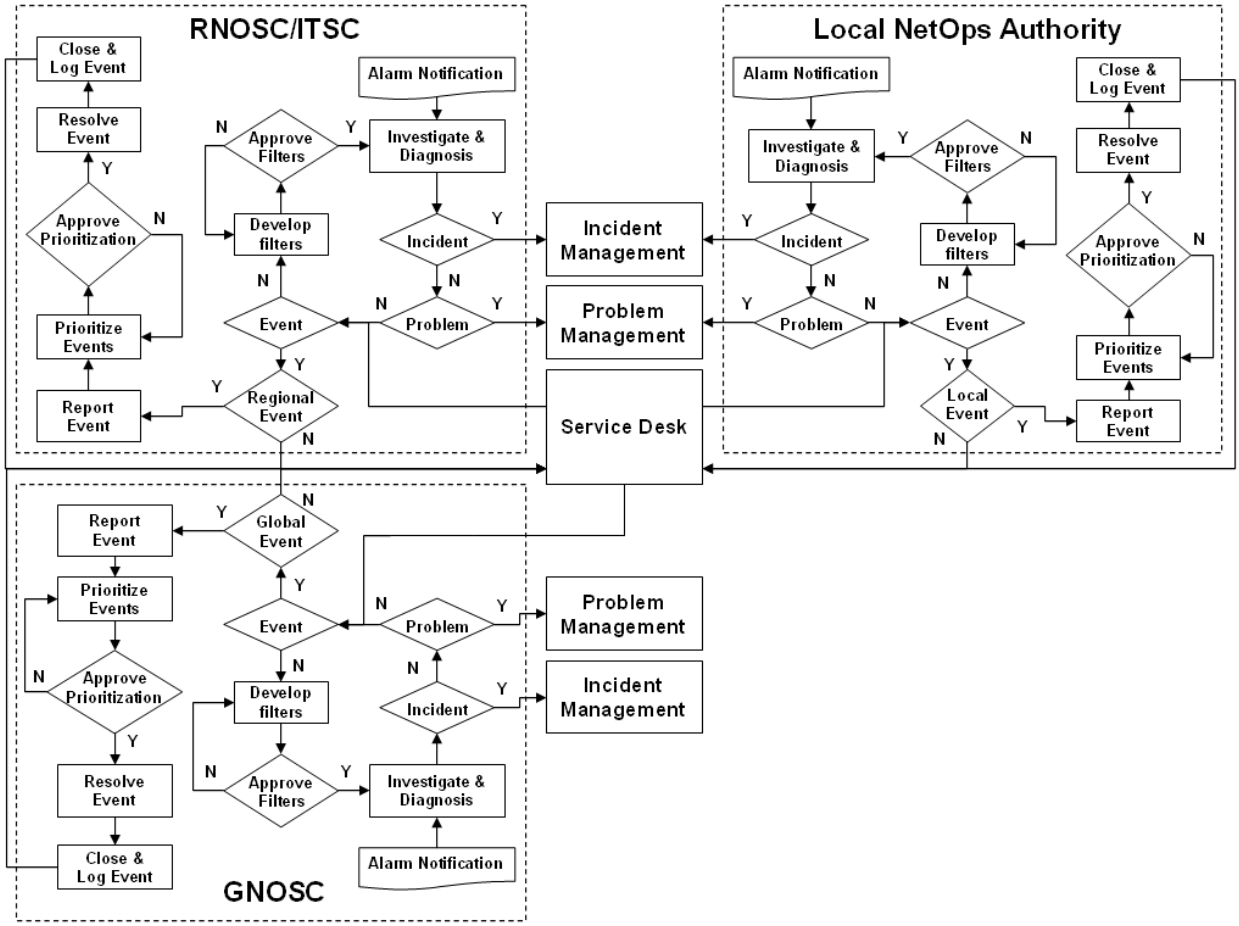


Figure 23 provides a high-level overview of the NGEN processes associated with event management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 23, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

Q.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the event management processes outlined in Figure 23 must be retained by the DON:

- **Approve filters.** The ability to direct NGEN operations is a management control function that shall be retained by the DON. The filters – or categorizations – will be used to assess whether an issue is an event, incident or problem as well as whether the issue should be addressed at the local, regional, or global NetOps authority.
- **Approve prioritization of events.** The ability to make decisions regarding the acceptance of risk is a management control function that shall be retained by the DON.

Q.2 Use Case: Quarantined Virus Alarm

Based on Figure 23, the process for resolving an event with an infected seat is:

- **Alarm notification.** A routine scan of the command's seats indicates a seat has been infected with a virus and it has been quarantined.
- **Investigate and diagnose issue.** Further examination of the alarm indicates only a single seat has been infected and the type of virus used to infect it.
- **Categorized as an event.** Since the infection is limited to a single seat, it is categorized as an event
- **Determine to be a local event.** The Detachment/Base G6 has the disinfection tools to deal with the virus and, therefore, the event is considered a local event to be dealt with by the local NetOps authority.
- **Report Event.** An initial report is submitted to higher NetOps authorities in accordance with CJCSM 6510.01.
- **Prioritize events.** All open events at the command are re-prioritized.
- **Approve prioritization of events.** The Detachment/Base G6 approves of the re-prioritization of open events.
- **Resolve event.** The event associated with the infected seat is resolved by disinfecting or re-imaging the hard drive of the seat.
- **Close event.** After scans of the seat indicate the virus is no longer present, the event is closed and a final report is submitted to higher NetOps authorities in accordance with CJCSM 6510.01.

This use case assumes local NetOps authorities are responsible for disinfecting seats infected with a virus. However, it is possible to perform this function remotely. If NGEN develops such a capability, then the event could be passed to either a regional or global NetOps authority – depending on which one operates the disinfection service. If it is not possible to successfully disinfect the seat, the event could then be passed back to the local NetOps authority to re-image the hard drive of the seat. In such a case, a loss of service would result and the event would have to be reclassified as an incident.

Q.3 Use Case: Collaboration Service Alarm

Based on Figure 23, the process for resolving an event with a collaboration service is:

- **Alarm notification.** A collaboration service has issued an alarm indicating the number of concurrent users has reached 85 percent of total capacity.
- **Investigate and diagnose issue.** Further examination of the alarm indicates usage has dramatically increased due to a recent operation (e.g., stand up of a Joint Task Force).
- **Categorized as an event.** Since current usage is not impacted, it is a categorized as an event.
- **Determine to be a regional event.** The RNOSC/ITSC operates collaboration services and, therefore, the event is considered a regional event to be dealt with by the regional NetOps authority.
- **Report event.** Event is reported to supported commands and higher NetOps authorities.
- **Prioritize events.** All open events at the RNOSC/ITSC are re-prioritized.
- **Approve prioritization of events.** The RNOSC/ITSC approves of the re-prioritization of open events.
- **Resolve event.** The RNOSC/ITSC works with commands to reduce usage of the service, coordinates with/obtains approval from the GNOSC to move some users temporarily to services hosted at other RNOSCs/ITSCs, etc. to prevent an incident from occurring.
- **Close event.** Close event after usage of the service has been reduced to a sustainable level. A request for change (RFC) could be issued to upgrade the collaboration service at the RNOSC/ITSC if there are concerns that a long-term solution is needed to prevent an incident.

This use case assumes regional NetOps authorities are responsible for collaboration services used by users within their region. However, it is possible that collaboration services are operated by the global NetOps authority. If NGEN develops such a capability, then the event outlined above is a global event and the GNOSC will be responsible for taking the appropriate actions to address it.

R Incident Management

Figure 24: NGEN Processes for Incident Management

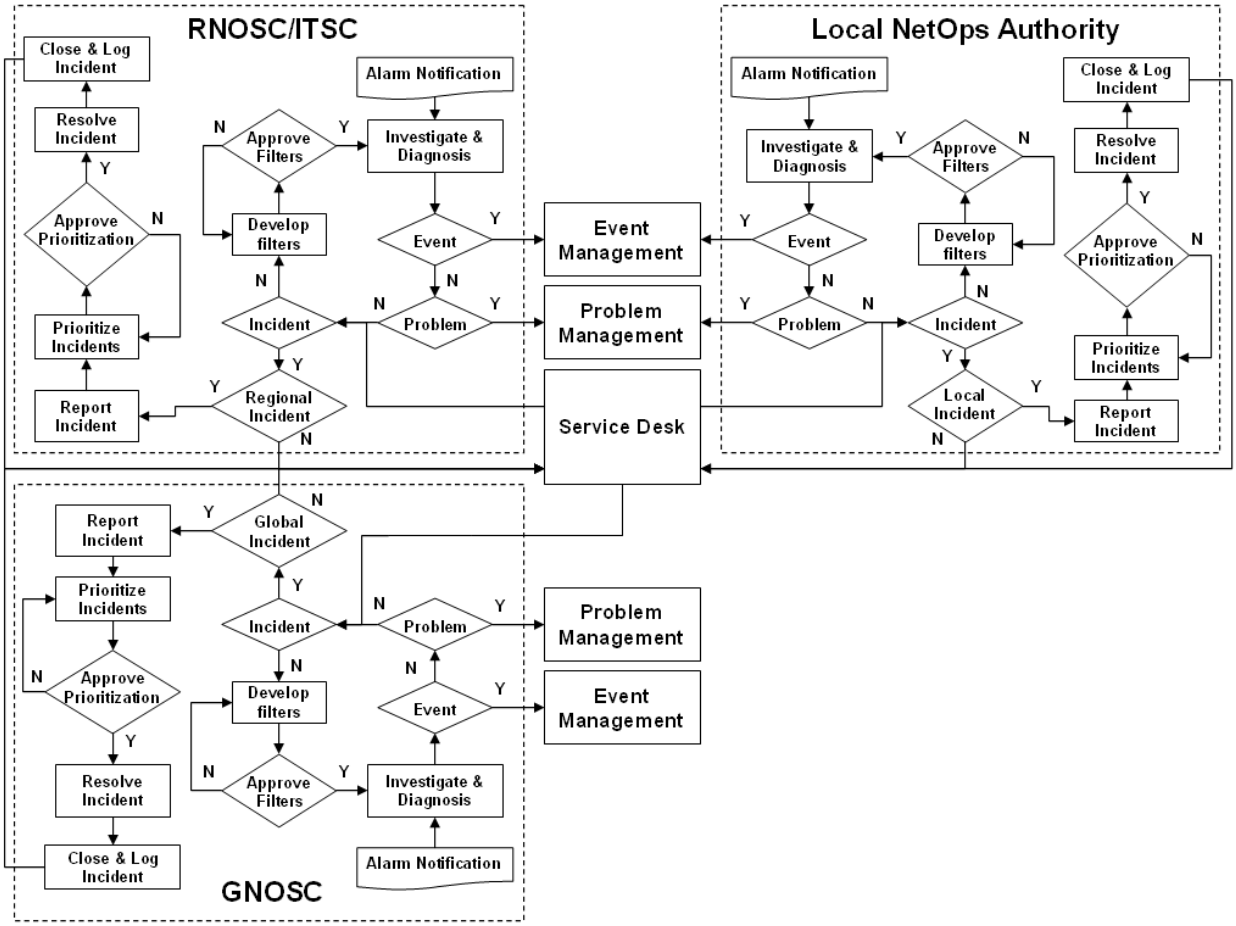


Figure 24 provides a high-level overview of the NGEN processes associated with incident management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 24, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

R.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the incident management processes outlined in Figure 24 must be retained by the DON:

- **Approve filters.** The ability to direct NGEN operations is a management control function that shall be retained by the DON. The filters – or categorizations – will be used to assess whether an issue is an event, incident or problem as well as whether the issue should be addressed at the local, regional, or global NetOps authority.
- **Approve prioritization of incidents.** The ability to make decisions regarding the acceptance of risk is a management control function that shall be retained by the DON.

R.2 Use Case: Virus Scanning Service Alarm

Based on Figure 24, the process for resolving an incident with an infected seat is:

- **Alarm notification.** A routine scan of the command's seats indicates the presence of a virus.
- **Investigate and diagnose issue.** Further examination of the alarm indicates 40 percent of the seats at a command have been infected by a virus.
- **Categorize as an incident.** Since the infection has spread to a significant number of seats, it is categorized as an incident.
- **Determine to be a local incident.** The Detachment/Base G6 has the disinfection tools to deal with the virus and, therefore, the incident is considered a local incident to be dealt with by the local NetOps authority.
- **Report incident.** An initial report is submitted to higher NetOps authorities in accordance with CJCSM 6510.01.
- **Prioritize incidents.** All open incidents at the command are re-prioritized.
- **Approve prioritization of incidents.** The Detachment/Base G6 approves of the re-prioritization of open incidents.
- **Resolve incident.** The Detachment/Base G6 quarantines all infected seats from the network and disinfects or re-images the hard drive of each seat.
- **Close incident.** After scans of the infected seats indicate the virus is no longer present, the seats are removed from quarantine and the incident is closed. A final report is submitted to higher NetOps authorities in accordance with CJCSM 6510.01.

This use case assumes local NetOps authorities are responsible for disinfecting seats. However, it is possible to perform this function remotely. If NGEN develops such a capability, then the incident should be passed to either a regional or global NetOps authority – depending on which one operates the disinfection service. If it is not possible to successfully disinfect the seats, the incident could then be passed back to the local NetOps authority to re-image the hard drive of the infected seats.

R.3 Use Case: Collaboration Service Alarm

Based on Figure 24, the process for resolving an incident with a collaboration service is:

- **Alarm notification.** A collaboration service has issued an alarm indicating the number of concurrent users has reached total capacity and users are being denied service.
- **Investigate and diagnose issue.** Further examination of the alarm indicates usage has dramatically increased due to a recent operation (e.g., stand up of a Joint Task Force).
- **Categorize as an incident.** Since some users are no longer able to access the service, it is a categorized as an incident.
- **Determine to be a regional incident.** The RNOSC/ITSC operates collaboration services and, therefore, the event is considered a regional event to be dealt with by the regional NetOps authority.
- **Report incident.** Incident is reported to supported commands and higher NetOps authorities.
- **Prioritize incidents.** All open incidents at the RNOSC/ITSC are re-prioritized.
- **Approve prioritization of incidents.** The RNOSC/ITSC approves of the re-prioritization of open incidents.
- **Resolve incident.** The RNOSC/ITSC works with commands to reduce usage of the service, coordinates with and obtains approval from the GNOSC to move some users temporarily to services hosted at other RNOSCs/ITSCs, etc.
- **Close incident.** Close incident after usage of the service has been reduced to a sustainable level. A request for change (RFC) could be issued to upgrade the collaboration service at the RNOSC/ITSC if there are concerns a long-term solution is needed to prevent another incident from occurring.

This use case assumes regional NetOps authorities are responsible for collaboration services used by users within their region. However, it is possible that collaboration services are operated by the global NetOps authority. If NGEN develops such a capability, then the event outlined above is a global event and the GNOSC will be responsible for taking the appropriate actions to address it.

S Problem Management

Figure 25: NGEN Processes for Problem Management

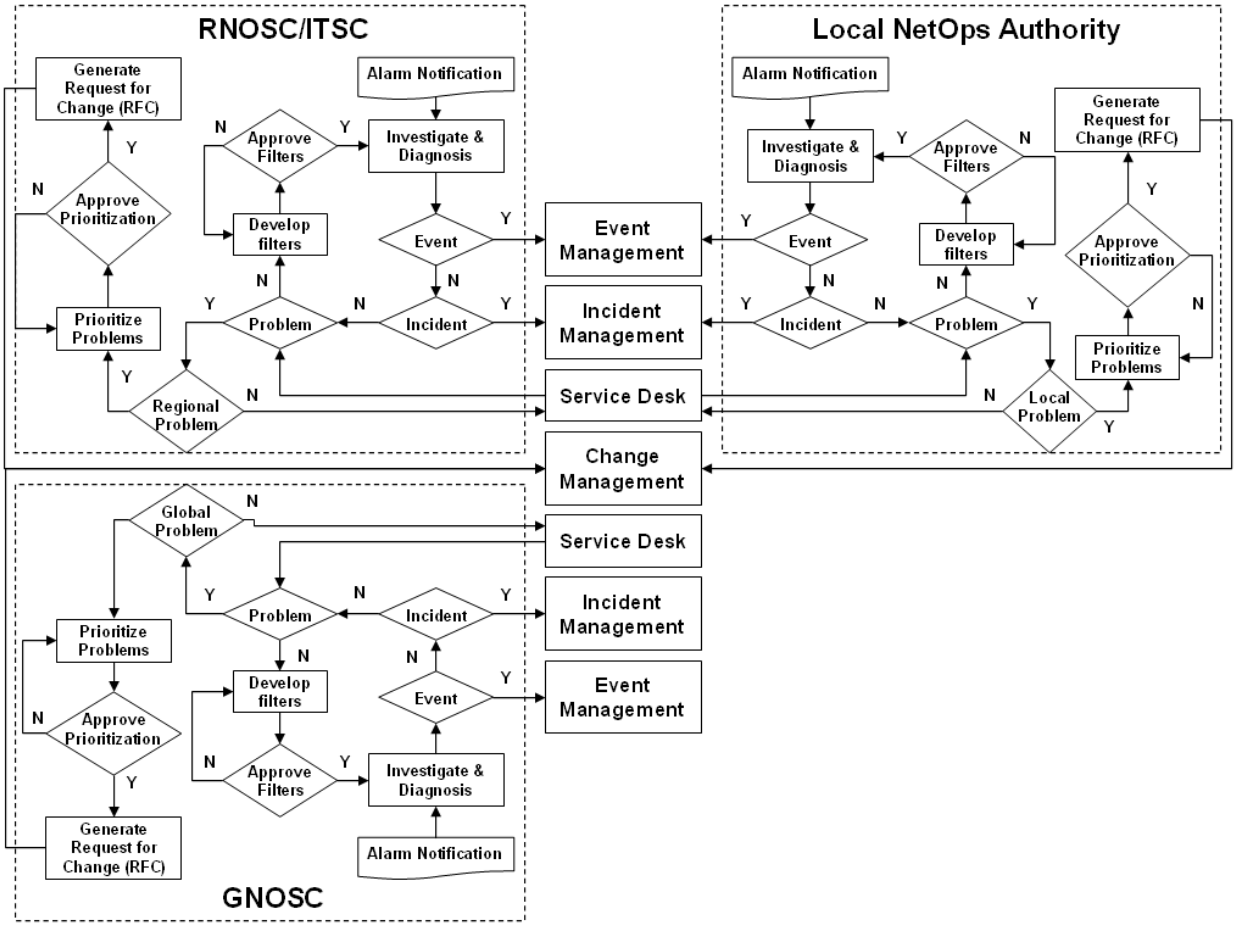


Figure 25 provides a high-level overview of the NGEN processes associated with problem management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 25, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

S.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the problem management processes outlined in Figure 25 must be retained by the DON:

- **Approve filters.** The ability to direct NGEN operations is a management control function that shall be retained by the DON. The filters – or categorizations – will be used to assess whether an issue is an event, incident or problem as well as whether the issue should be addressed at the local, regional, or global NetOps authority.
- **Approve prioritization of problems.** The ability to make decisions regarding the acceptance of risk is a management control function that shall be retained by the DON.

S.2 Use Case: Virus Scanning Service Alarm

Based on Figure 25, the process for resolving a problem that resulted in the infection of NGEN seats:

- **Alarm notification.** A routine scan of the command's seats indicates the presence of an intrusion.
- **Investigate and diagnose issue.** Review of similar incident records indicates a pattern of like infections at this command and others. Further examination indicates seats at various commands have previously been infected by the same virus due to an inability to scan hypertext transfer protocol secure (HTTPS) content.
- **Categorize as a problem.** Since similar incidents are reoccurring and the viruses were introduced via a design flaw, it is categorized as a problem.
- **Determine to be a global problem.** The GNOSC is responsible for operating security scanning services and, therefore, the problem is considered a global problem to be dealt with by the global NetOps authority.
- **Prioritize problems.** All open problems at the GNOSC are re-prioritized.
- **Approve prioritization of problems.** The GNOSC approves of the re-prioritization of open problems.
- **Generate a Request for Change (RFC).** The GNOSC generates a RFC to provide the capability to scan HTTPS content and, due to the nature of this vulnerability and risk to operations, the RFC is expedited as an emergency change.

S.3 Use Case: Collaboration Service Alarm

Based on Figure 25, the process for resolving a problem with a collaboration service is:

- **Service Desk.** A number of users are reporting they are not able to access the collaboration service.
- **Investigate and diagnose issue.** Further examination of the reports indicate that an upgrade to the users' seats is not compatible with the collaboration service.
- **Categorize as a problem.** Since users are no longer able to access the service due to an issue with the design/upgrade and incidents are re-occurring without an acceptable permanent fix, it is a categorized as a problem.

- **Determine to be a global problem.** While the RNOSC/ITSC operates collaboration services, the seat configurations are a global NetOps responsibility. Therefore, the GNOSC is the NetOps authority responsible for addressing the problem.
- **Prioritize problems.** All open problems at the GNOSC are re-prioritized.
- **Approve prioritization of problems.** The GNOSC approves of the re-prioritization of open problems.
- **Generate a Request for Change (RFC).** The GNOSC generates a RFC to address the interoperability issue with the upgraded seats and the collaboration service.

T Service Desk Operations

Figure 26: NGEN Processes for Service Desk Operations

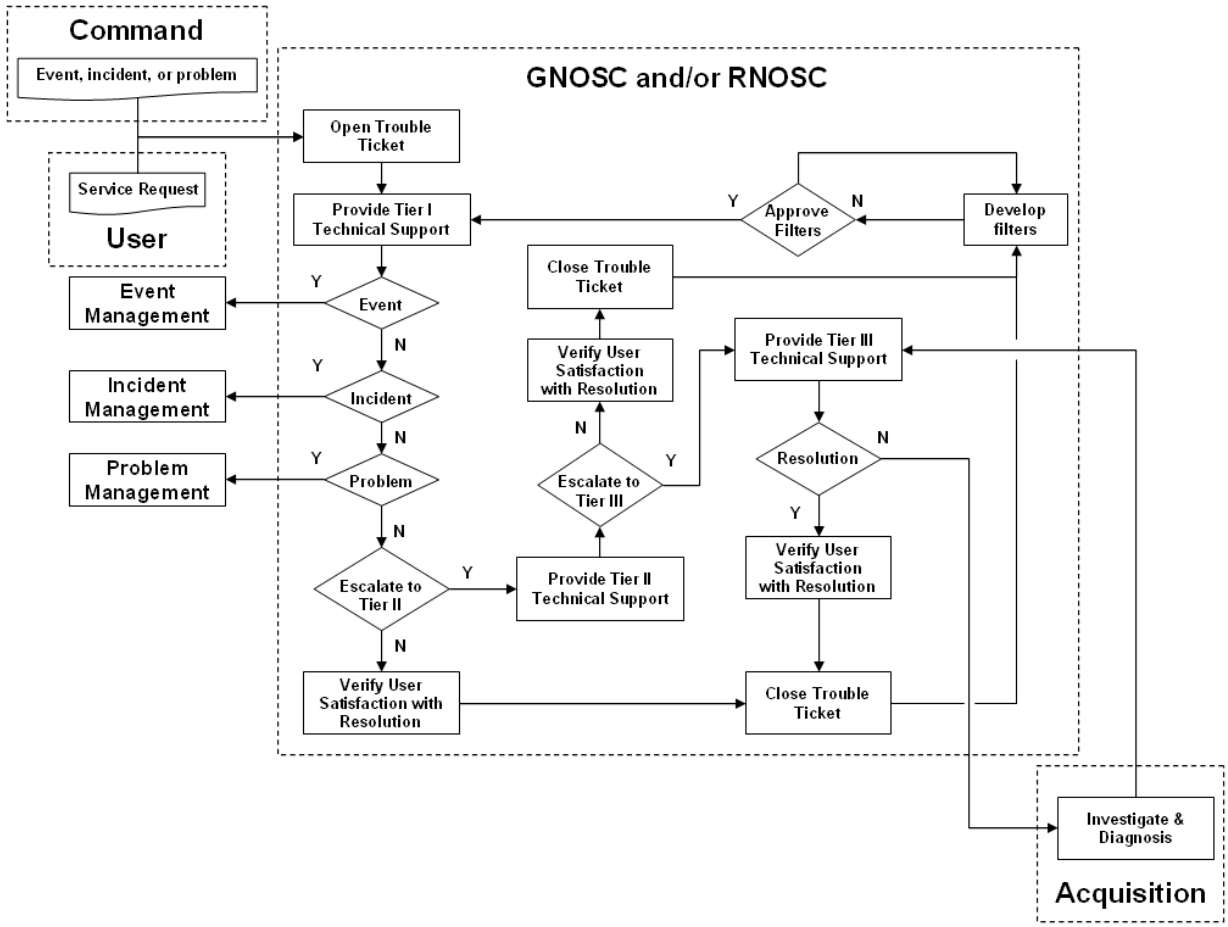


Figure 26 provides a high-level overview of the NGEN processes associated with service desk operations, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 26, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

T.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the service desk processes outlined in Figure 26 must be retained by the DON:

- **Approve filters.** The ability to direct NGEN operations is a management control function that shall be retained by the DON. The filters – or categorizations – will be used to assess whether an issue is an event, incident or problem as well as whether the issue should be addressed at the local, regional, or global NetOps authority.

T.2 Service Tiers

NGEN service desk support is divided into three tiers of service:

- **Tier I – Help Desk Analyst**. Tier I personnel are expected to:
  - Field calls/e-mails and work with customers until the trouble ticket is resolved
  - Create user accounts and maintain user account groups
  - Re-set account passwords
  - Maintain Exchange accounts and distribution lists
  - Escalate trouble tickets that cannot be immediately resolved with their own expertise
- **Tier II – System Technician**. Tier II personnel are expected to:
  - Provide the support, knowledge and tools that enable Tier 1 personnel to provide efficient end-user support
  - Resolve all server operations issues
  - Support mailbox/folder tape restoration
  - Provide web site maintenance and support
  - Escalate trouble tickets that cannot be resolved with their own expertise
- **Tier III – System Engineer**. Tier III personnel are expected to:
  - Assist Tier II personnel to resolve issues and develop solutions
  - Perform system analysis
  - Support performance optimization
  - Support mailbox and public folder recovery
  - Escalate trouble tickets that cannot be resolved with their own expertise to subject matter experts

The NGEN engineers and architects within the acquisition community possess in-depth subject matter expertise and, while not part of the normal support team, may be called on to help with trouble tickets that cannot be resolved by Tier III personnel.

T.3 Use Case: New User Request

Based on Figure 26, the process for the service desk resolving a new user request is:

- **Receive of new user request.** A validated new user request is received from a command.
- **Open trouble ticket.** Create a trouble ticket for the new user request.
- **Provide Tier I technical support.** Service desk personnel request validation from the appropriate NetOps authority and creation of the PKI certificate.
- **The trouble ticket is not an event.** A new user request is not an event.
- **The trouble ticket is not an incident.** A new user request is not an incident.
- **The trouble ticket is not a problem.** A new user request is not a problem.
- **Escalation to Tier II is not required.** Tier I support is sufficient to resolve the service request.
- **Verify user satisfaction.** Verify the user has received his/her common access card (CAC) and has been able to access NGEN services.
- **Close trouble ticket.** Close the trouble ticket for the new user request.

T.4 Use Case: Password Reset

Based on Figure 26, the process for the service desk resolving a request to reset a password:

- **Receive password reset request.** The user calls or e-mails the service desk with a request to reset a password.
- **Open trouble ticket.** Create a trouble ticket for the password reset request.
- **Provide Tier I technical support.** Service desk personnel reset the user's password, provide the user with a temporary password, and instruct the user to change their password immediately.
- **The trouble ticket is not an event.** A password reset request is not an event.
- **The trouble ticket is not an incident.** A password reset request is not an incident.
- **The trouble ticket is not a problem.** A password reset request is not a problem.
- **Escalation to Tier II is not required.** Tier I support is sufficient to resolve the service request.
- **Verify user satisfaction.** Verify the user has reset their password.
- **Close trouble ticket.** Close the trouble ticket for the password reset request.

T.5 Use Case: Request to Recover an E-mail

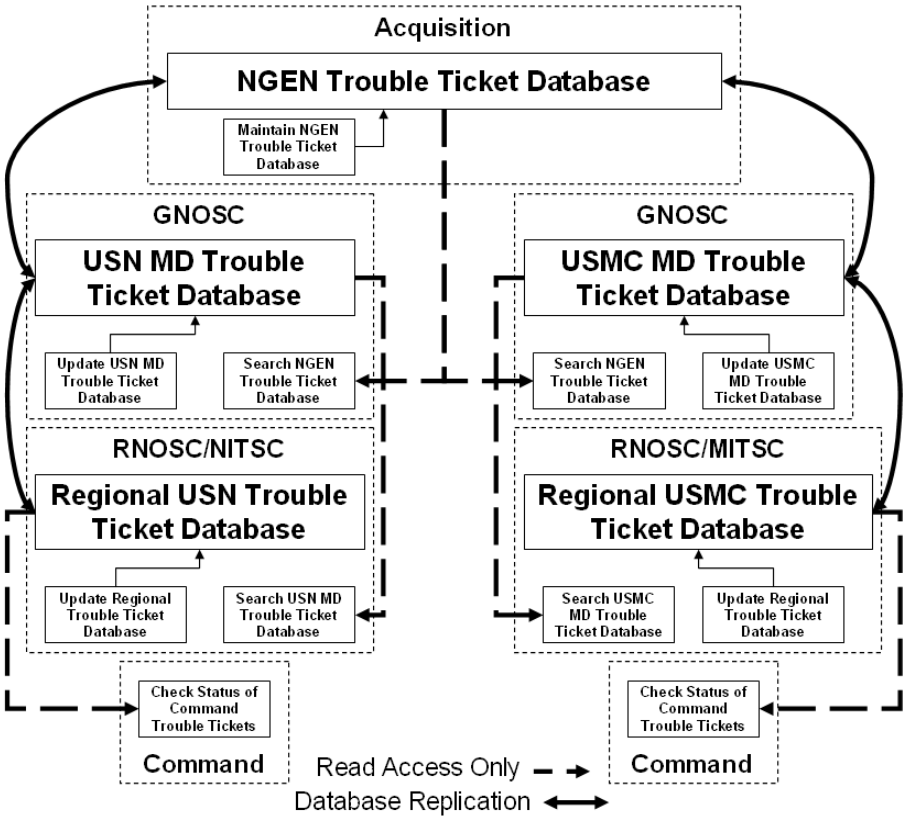
Based on Figure 26, the process for the service desk to resolve a request to recover an e-mail is:

- **Receive password reset request.** The user calls or e-mails the service desk about an important e-mail that was accidentally deleted.
- **Open trouble ticket.** Create a trouble ticket for the request.
- **Not a Tier I issue.** Tier I technical support services receives an e-mail recovery request.
- **The trouble ticket is not an event.** A request for e-mail recovery is not an event.
- **The trouble ticket is not an incident.** A request for e-mail recovery is not an incident.
- **The trouble ticket is not a problem.** A request for e-mail recovery is not a problem.
- **Escalation to Tier II is required.** Tier I support is not sufficient to resolve the service request.
- **Provide Tier II technical support.** The Tier II technician locates the correct back-up tape, recovers the e-mail message, and restores it to the user's mailbox.
- **Close trouble ticket upon resolution.** Close the trouble ticket for the request to recover e-mail after the user verifies receipt of the requested e-mail message.

T.6 Federated Trouble Ticket Management System

Figure 27 depicts a federated NGEN trouble ticket management system. With this federated architecture, the technical design authority maintains a master trouble ticket database that contains trouble tickets from both the USN and USMC MDs. Each NGEN MD then maintains its own trouble ticket system at the GNOSC, which synchronizes its trouble tickets with the master database. Regional RNOSCs/ITSCs also maintain their own regional trouble ticket system, which synchronizes its trouble tickets with the larger databases at the GNOSC. The federated trouble ticket system is scalable and can be integrated with trouble ticket systems of other Management Domains (DISA, IT-21, WFNS, etc.) under common standards. The replication of trouble tickets between these databases allows each NetOps authority to maintain their respective portions of the master trouble ticket database and the replication process ensures any changes are quickly reflected in trouble ticket systems for the MD and the master NGEN trouble ticket database. Integration allows for coordinated efforts to resolve problems when they extend beyond NGEN. Individual commands need visibility into the status of their open trouble tickets and, therefore, require read-only access to the trouble ticket database.

Figure 27: Federated Trouble Ticket Management System for NGEN



U Access Management

Figure 28: NGEN Processes for Access Management

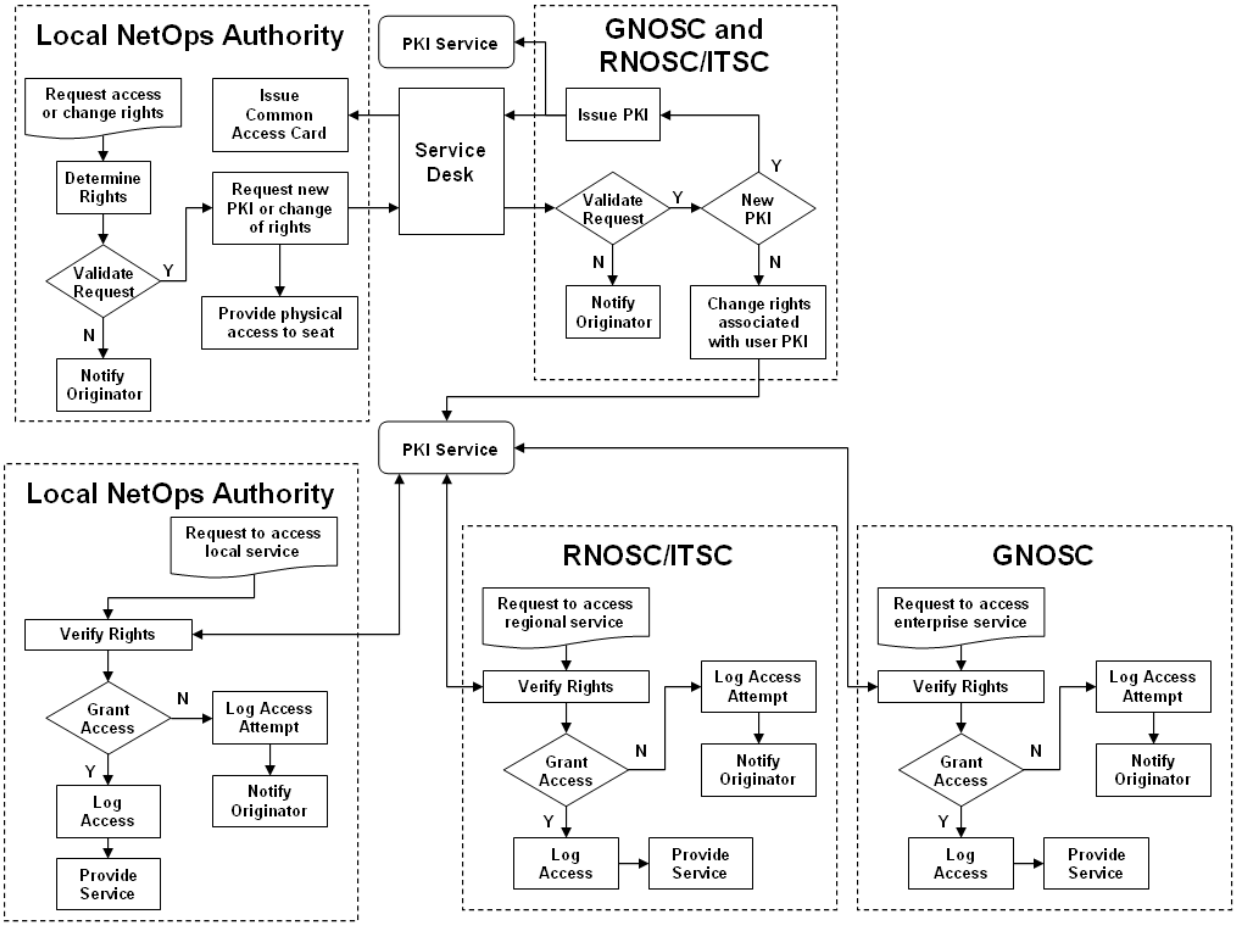


Figure 28 provides a high-level overview of the NGEN processes associated with access management, which will continue to be refined as NGEN is developed and procured. Each diamond represents a decision point and each box represents a task. It is important to realize that, while not shown in Figure 28, there could be a series of sub-tasks or additional processes associated with each decision point or task. The next section identifies the NetOps management control functions that, according to the criteria outlined in Annex C, shall be retained by the DON. It is beyond the scope of this CONOPS to identify management control functions associated with governance or acquisition.

U.1 NGEN NetOps Authority

The following NetOps decision points or tasks within the access management processes outlined in Figure 28 must be retained by the DON:

- **Validate Request.** Approval authority over NGEN operations is a management control function that shall be retained by the DON. The Command G6/N6 must validate the need for a user to gain access to NGEN and the digital rights the user should receive. Since the GNOSC retains NetOps OPCON and TACON over the PKI service, it must validate the command's request.
- **Grant Access.** Approval authority over NGEN operations is a management control function that shall be retained by the DON. Only the DON data/service owner can grant access to their data/services. It is important to recognize this does not necessarily mean a person has to approve every access request. The data/service owner decides which rights are required to access the data/service (e.g., only command users, members of a COI, etc.). After a user's rights have been verified with the PKI service, the rules established by the DON data/service owner are used to determine whether the user can access the data/service.

U.2 Use Case: New User Request

Based on Figure 28, the process for granting a new user access to NGEN is:

- **User generates a request for access.** A user – who currently does not have access to NGEN – completes a form to request access.
- **Determine appropriate rights.** The digital rights of the user are determined based on the command, user's responsibilities, and any special requests.
- **Command validates request.** The Command G6/N6 validates the request for access and the associated digital rights. If the Command G6/N6 does not validate the request, the user is notified and can generate another request.
- **Validates request.** The GNOSC or RNOSC/ITSC validates the command request for user access. If the request is not validated, the user is notified and can generate another request.
- **New PKI certificate is required.** Since this is a new user request, a new PKI certificate needs to be issued.
- **Issue PKI certificate.** A new PKI certificate is issued, via the PKI service, with the validated digital rights associated with it.
- **Issue CAC.** The command – or more commonly the base – issues a CAC to the user.

The user can access NGEN from any of its seats using their CAC card. This process will be used to grant NGEN access to military personnel, DON civilians, and contractors that support the DON or military commands.

U.3 Use Case: Change Rights of Existing User

Based on Figure 28, the process for changing user access rights is:

- **User generates a request for rights.** A user – who already has access to NGEN – fills out a form to request to change his or her digital rights.
- **Determine appropriate rights.** The digital rights of the user are determined based on the command, user's responsibilities, and any special requests.
- **Command validates request.** The Command G6/N6 validates the request for additional digital rights. If the Command G6/N6 does not validate the request, the user is notified and can generate another request.
- **GNOSC validates request.** The GNOSC, who exerts NetOps OPCON and TACON over the PKI service, validates the command request for additional user rights, which may require obtaining approval from the data/service owner. If the GNOSC does not validate the request, the user is notified and can generate another request.
- **No new PKI certificate is required.** Since the user already has NGEN access, he or she already has a PKI certificate.
- **Change digital rights associated with the user's PKI.** The GNOSC adds the requested digital rights to those already associated with the user's PKI.

This process will be used to change access rights of military personnel and DON civilians during a change of duty station. This process also supports the changing of digital rights in support of emerging operational requirements (e.g., the establishment of a JTF and associated COI).

While the above use case outlines the addition of digital rights, the same process can be used to revoke digital rights. For example, after a user separates from a command, the command will submit a request to have the user's access rights to command data/services removed. Once the command has validated the revocation of certain digital rights of a user, the GNOSC does not need to validate the request and should promptly revoke the user's rights.

U.4 Use Case: User Access to Data/IT Services

Based on Figure 28, the process for accessing data/services is:

- **User requests access to data/IT service.** The user attempts to access the data/IT service using their NGEN account.
- **Verify rights.** The owner of the data/IT service verifies the user's digital rights with the PKI service.
- **Log access.** Log the user, the user's rights, whether access was granted, and the date-time group of the access.
- **Provide data/IT service.** If the user has the rights to access the data or use the IT service, access is granted. Otherwise, access is denied and the user is notified.

This process is used for attempts to access data/IT services hosted by individual commands, regional IT services or enterprise-level services hosted by EITCs. Individual commands may be responsible for maintaining databases (e.g., logistics, casualty reports, etc.) and external users may need to modify or read portions of it. These rights are associated with the user's PKI and can be used by the IT service to determine the level of access of the user (e.g., read access, read access to portions of the database, write access, write access to portions of the database, etc.). RNOSCs/ITSCs may support collaboration services and the digital rights associated with a user could be used to determine which COIs he or she is able to participate/interact with. EITCs maintain enterprise-level IT services and the digital rights associated with the user will allow use of services and/or access to their data.